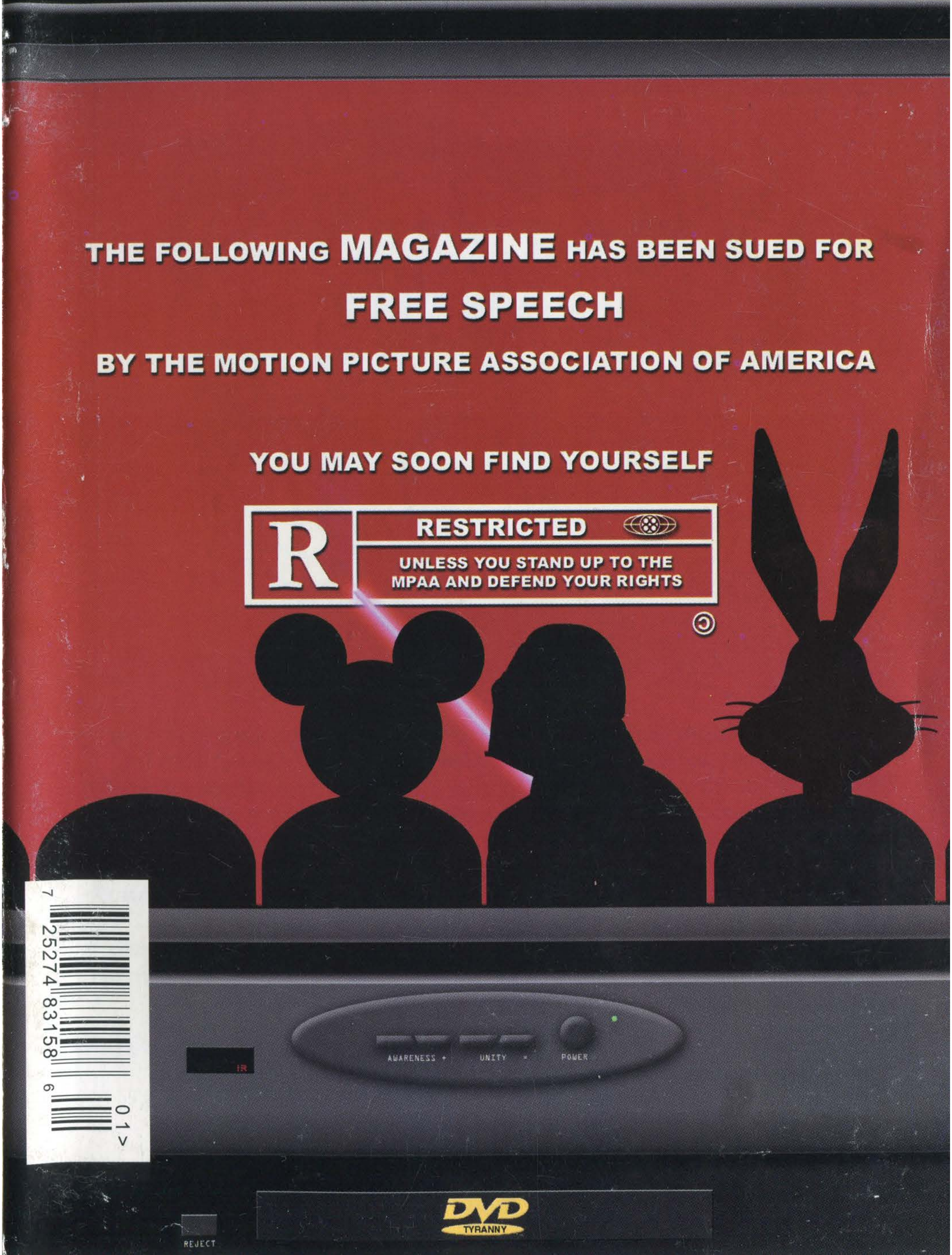
2600

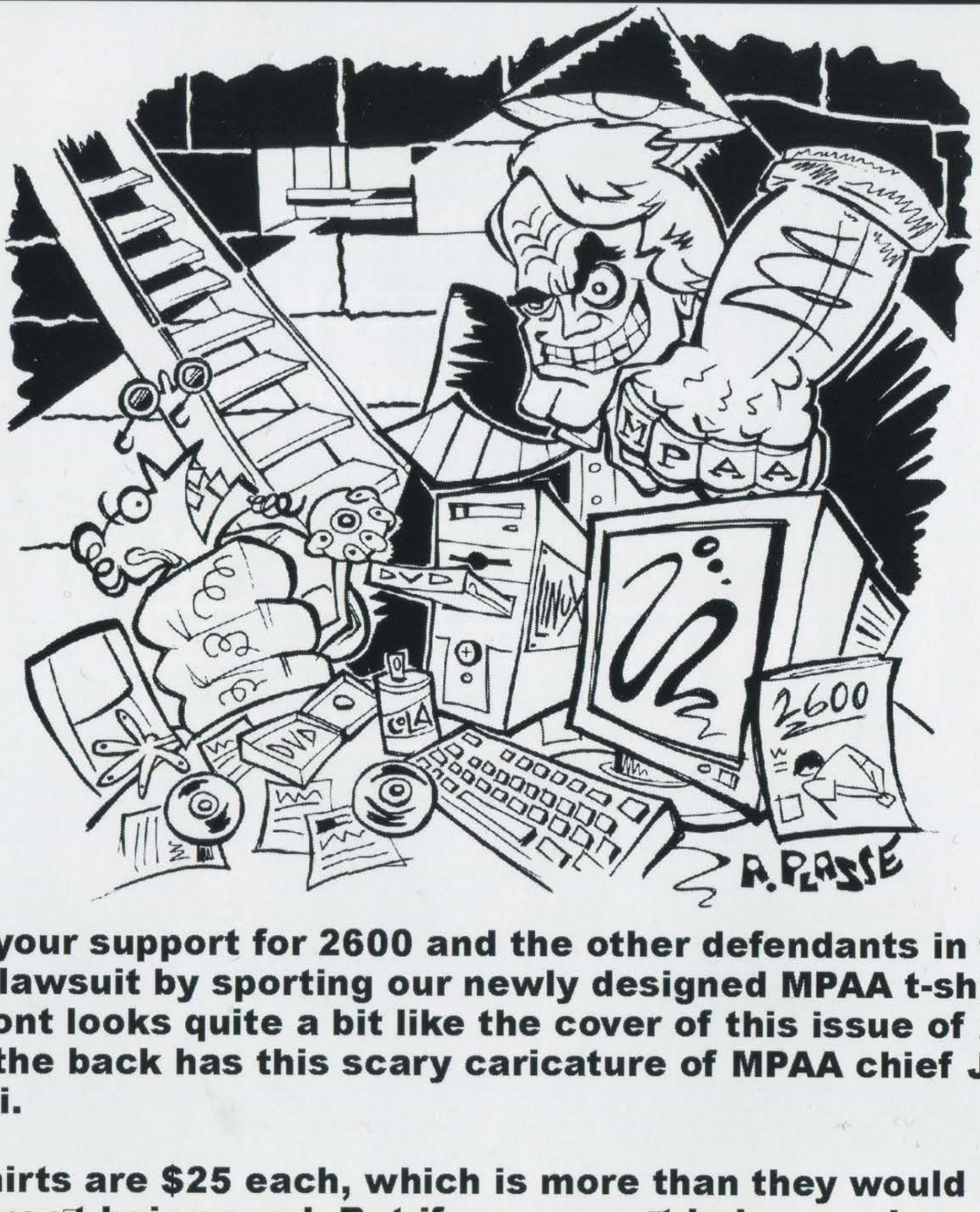
The Hacker Quarterly

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


THE FOLLOWING MAGAZINE HAS BEEN SUED FOR
FREE SPEECH
BY THE MOTION PICTURE ASSOCIATION OF AMERICA
YOU MAY SOON FIND YOURSELF
R
RESTRICTED
UNLESS YOU STAND UP TO THE MPAA AND DEFEND YOUR RIGHTS
AWARENESS +
UNITY =
POWER
DVD
TYRANNY
REJECT

7 25274 83158 6 01>

TIME TO FIGHT BACK



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

The shirts are $25 each, which is more than they would be if we weren□t being sued. But if we weren□t being sued, we wouldn□t have made the shirts! The extra money will go into our defense fund and hopefully prevent this kind of crap from happening again.

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

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

PLEASE SELECT THE ARTICLE YOU WISH TO SUE US OVER*

*resist

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

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
TANKEDUPQUEER

Cover Design
PIP, The Chopping Block Inc.

Office Manager
Tampruf

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

Webmaster: **Macki**

Network Operations: **CSS, Izaac**

Video Production: **Porkchop**

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

IRC Admins: **autojack, ross**

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

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

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

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

Copyright (c) 2000 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**

The Next Chapter

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

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

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

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

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

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

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

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

When the DVD encryption was defeated, hackers, as is their instinct, told the world and made the source code available. This resulted in threats being made against them for daring to figure it out. As a show of support, we posted the source code on our web site, as did many others. We actually thought reason would prevail - until one day in late December webmaster@2600.com was served (via email) with legal papers from the DVD Copy Control Association. We thought it was pretty funny that a lawsuit could be emailed and even funnier still that they actually believed they could prevail in such a manner. We don't even have a working DVD player and here they were accusing us of piracy. Not to mention the fact that we weren't even involved in figuring it out in the first place.

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

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

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

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

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

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

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

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

It sounds absurd because it *is* absurd. And that is precisely why we're not going to back down on this and why others should take up the fight before things get any worse. The world the MPAA and the megacorporations want us to live in is a living hell. They are motivated by one factor alone and that is greed. If they can make you buy the same thing multiple times, they will. If they can control the hardware as well as the software, they will. If they can prevent equal access to technology by entities not under their umbrella, they will. And you can bet that if they have to lie, cheat, and deceive in order to accomplish this, they most definitely will.

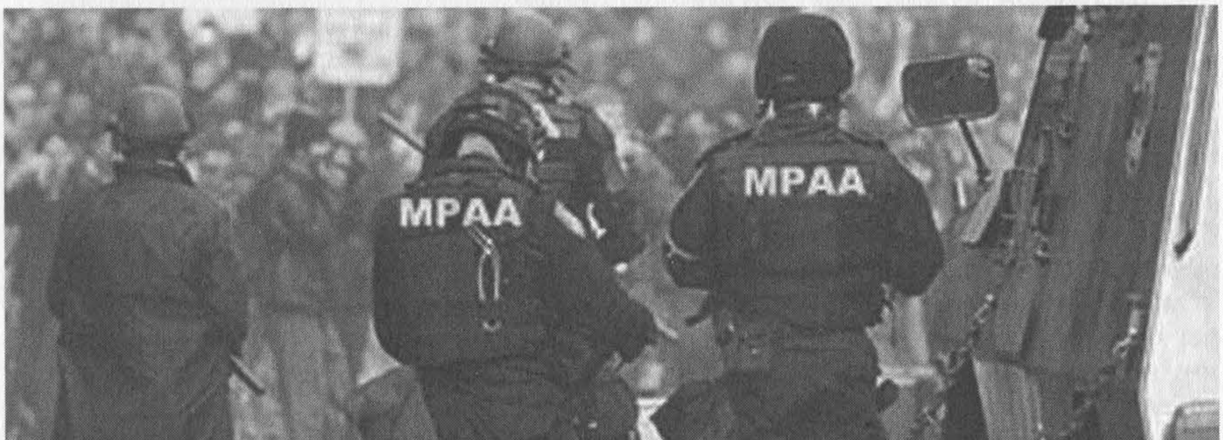
Let's take a look at what the MPAA has been saying publicly. When the injunction was granted against us, they called it a victory for artists and a strike against piracy. The newspapers and media outlets - most of them owned by the same companies that are suing us - dutifully reported just that. But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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

A TASTE OF FREEDOM

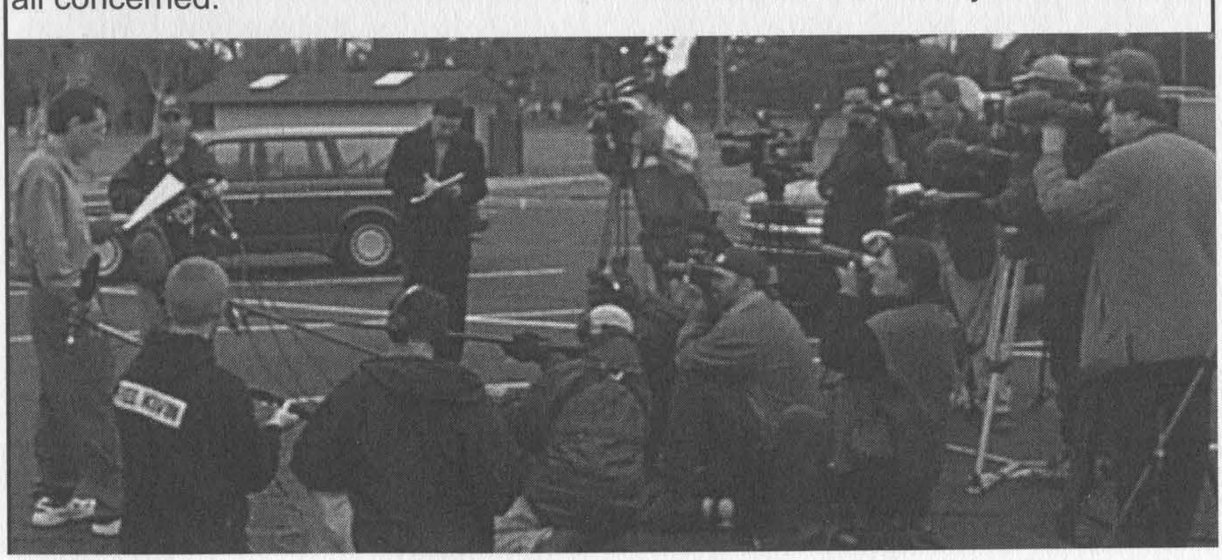
by Kevin Mitnick

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

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

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

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



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

On The Inside

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

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

Conditional Freedom

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

The Senate

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

Compare those feelings to the way I was treated like shit and like I was the scum of the earth while in federal prison. Guards patted me down at any time. I was bound and shackled to move 25 feet (to an MRI device on a truck parked at the curb outside the prison) just 48 hours before my release. The disrespect by the majority of federal prison staff members is shocking. I was strip searched after each visit from friends and family. During these visits, I had to time my request to use the bathroom on the half-hour, only to have my request refused on a guard's whim. I was treated like a bank robber, drug dealer, or murderer. And six weeks later I was in a blue pinstripe suit in front of the U.S. Senate.

New York

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

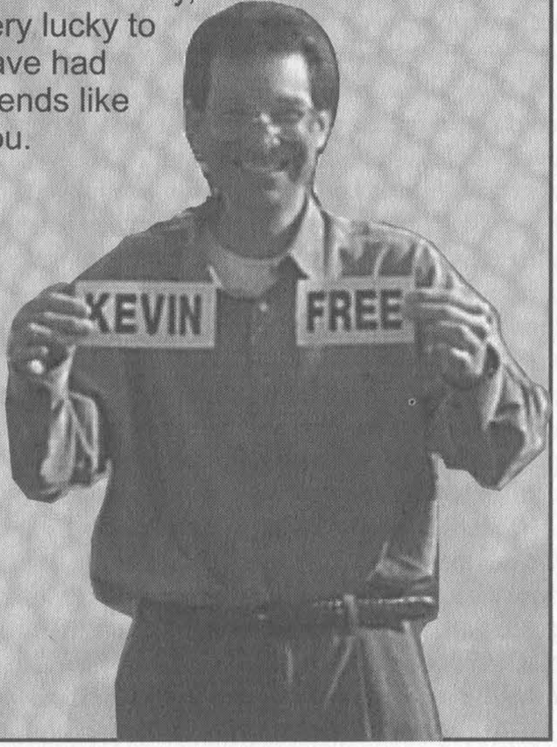
Emmanuel was at the *Crier Today* filming, and we spent some time sightseeing before we went to the lobby of the Citicorp building. It was my first time in New York, my first *2600* meeting, and it was the best time I've had since I was released from jail. I greatly enjoyed meeting many of my supporters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

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

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

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

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



HOW TO STAY A SYSADMIN

by Shade

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

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

The pitfalls of technical gurus are not unique. I've seen the patterns repeated over and over, yet even the author has a hard time avoiding the same mistakes. We think alike. It's getting so bad it's showing up on SNL. Techies seem to be able to keep other techies up to date on the latest kernel level, version release, or service pack but never communicate about the more mundane aspects, like hacks on keeping the ideal job.

Getting hired for the job is beyond the scope of this article. This is about keeping it. Gather 'round young and old, for I pull no punches here.

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

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

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

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

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

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

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

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

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

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

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

MILITARY COMPUTER SECRETS

by Suicidal

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

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

Securing Web Sites With ASP

by guinsu

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

Make Sure Only Valid Users Can Get In

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

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

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

The way you put information in a session object is simple:

```
Session("User_ID")= 12345
```

You can create items in the session on the fly without declaring them and pull them out just as easily:

```
Temp_str=Session("First_Name")
```

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

Now that I have covered the groundwork of the session, here is how it can be put to use. A user submits a form on a login page with a user name and password. Then a verification page compares those values to the values stored in the database. If a user is determined to be a valid user we have a line like this:

```
Session(“Authenticated”)=”TRUE”
```

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

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

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

Making Sure Valid Users Can See Only Their Information

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

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

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

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

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

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

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

```
Request.ServerVariables(“HTTP_REFERER”).
```

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

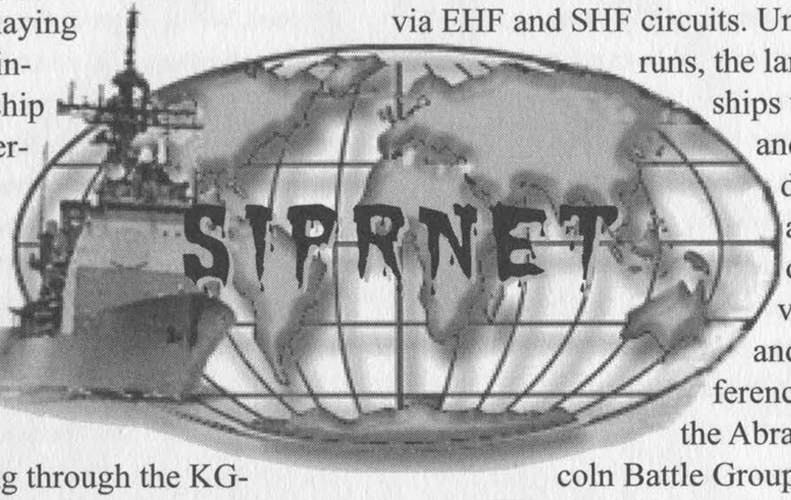
http://w3.one.net/~jhoffman/sqltut.htm Also, I am sure I missed a few holes that I am just not aware of. So do not take this as the end all and be all of securing sites in code.

www.2600.com

STILL MORE ON SIPRNET

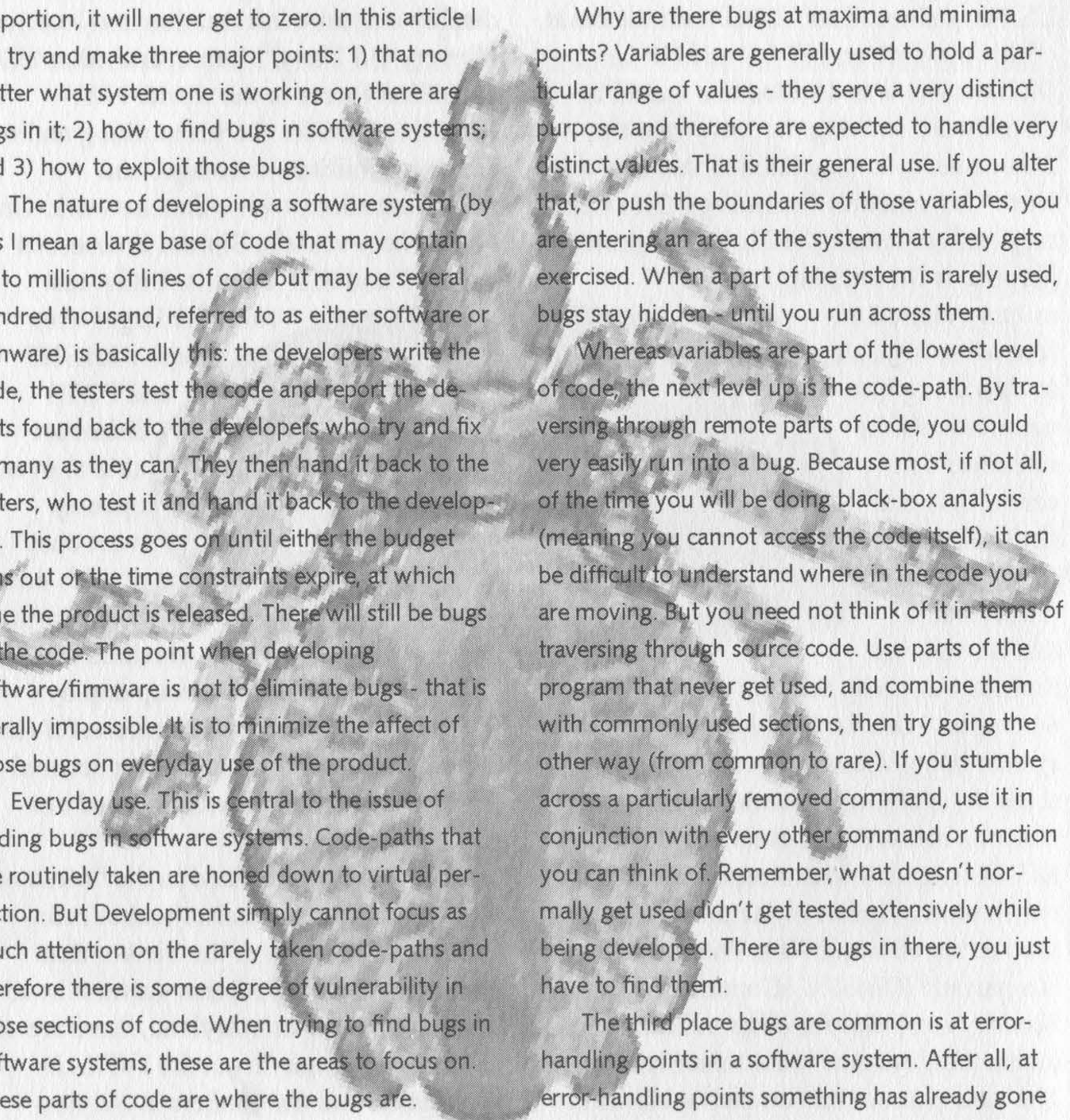
by Phrostbyte

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



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

Finding and Exploiting Bugs



by Astroman66

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

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

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

How to Find Bugs

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

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

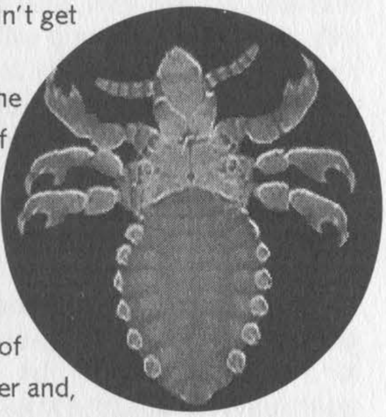
Whereas variables are part of the lowest level of code, the next level up is the code-path. By traversing through remote parts of code, you could very easily run into a bug. Because most, if not all, of the time you will be doing black-box analysis (meaning you cannot access the code itself), it can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

The third place bugs are common is at error-handling points in a software system. After all, at error-handling points something has already gone wrong and now the system must recuperate from that error. This is not always a clean process. There are a number of things that could happen if the process fails, from locking the system to dropping you out of the program to the shell. Try generating errors, but from an odd perspective. Say a certain password program fires up when your computer is undisturbed for five minutes. That this little program must look up your password makes it interesting enough, but what happens if some error should occur while it is doing so? Is this program, or part of a larger system, designed to handle all combination of characters given it? What about system (or reserved) character combinations? What about maxing out the arrays? It's worth a try....

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

Exploiting Bugs

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



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

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

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

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

Some Points to Keep in Mind

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

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

Use Boundary Testing to push variables to the limit.

Try exercising remote code-paths.

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

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

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

ALL ABOUT SECURID

by magus
securid@terrorists.net

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

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

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

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

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

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

Each token has an eight digit serial number stamped on the back, right next to "Please return to Security Dynamics... yadda yadda." This is used to track the token in the ACE (Access Control Electronics) server, enable/disable it, unbind it from someone's account, etc., etc. Each token also has a self-destruct date. Contrary to the popular beliefs of *Mission Impossible* junkies, it will not detonate a small thermite charge on this date - it merely ceases to work and obstinately displays "Sd Inc" on its display, or merely flashes a single dot, or both. Dead SecurID's have been known to start doing *something* with strong electrostatic discharge - they count, but not in the way they are supposed to. They are fairly resistant to such discharge, although I've only tested on the older cards and the newer key fobs. If anyone has tried HERFing one, I'd like to hear the results. Some people have theorized that they also self-destruct if opened - I maintain it's just really hard to open one without breaking it [grin]. Then again, I've only tried this on older cards.

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

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

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

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

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

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

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

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

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

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

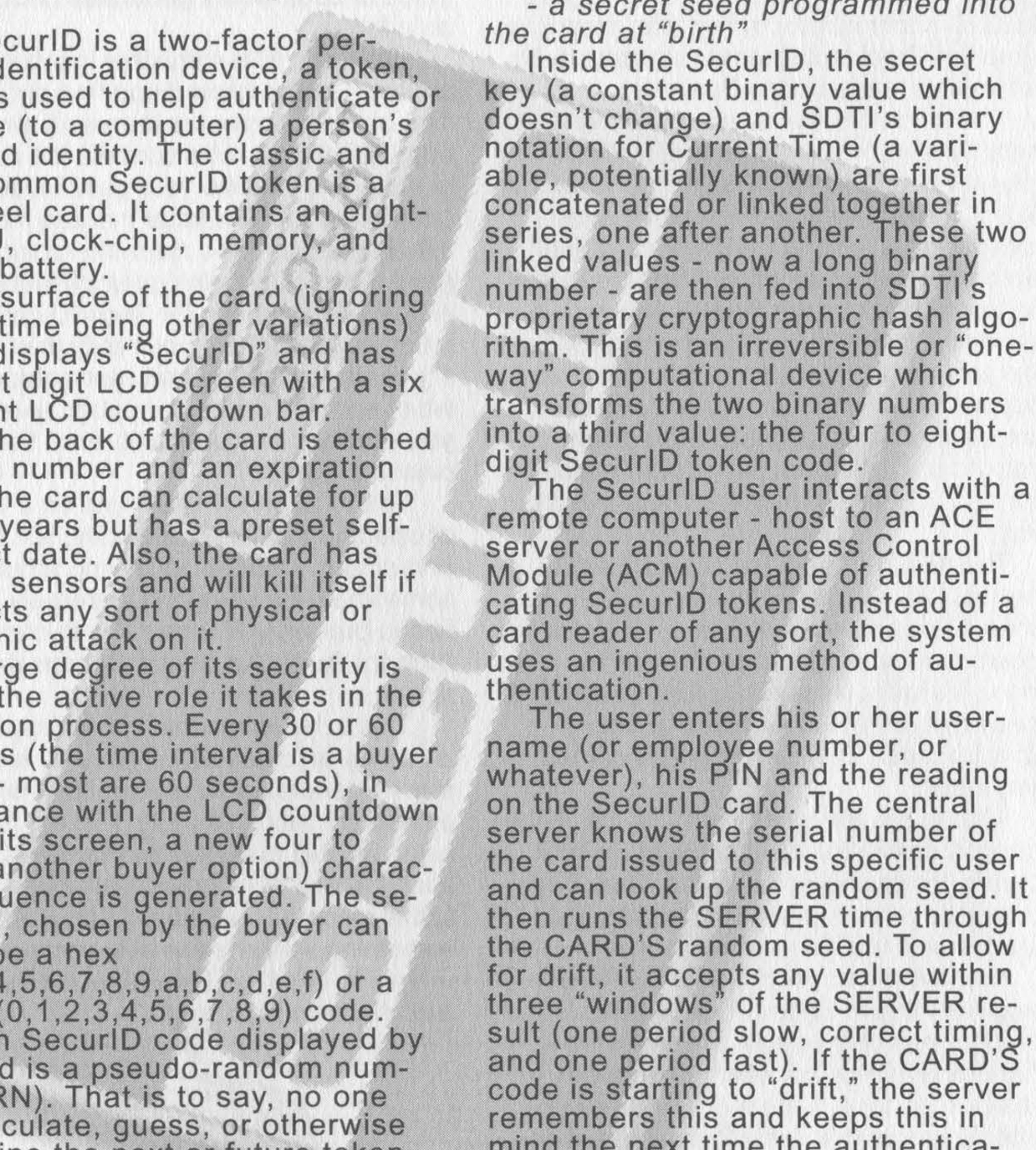
This is by no means a complete work - it is merely an overview of SecurID technology as generated by my memory, which is admittedly failing as a result of my fool brain being unable to adapt itself to run off caffeine instead of glucose. If anyone wants technical details on administering ACE or something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

SecurityDynamics

SECURID

by xenox

xenox9@hushmail.com



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

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

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

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

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

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

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

- the non-secret time

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

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

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

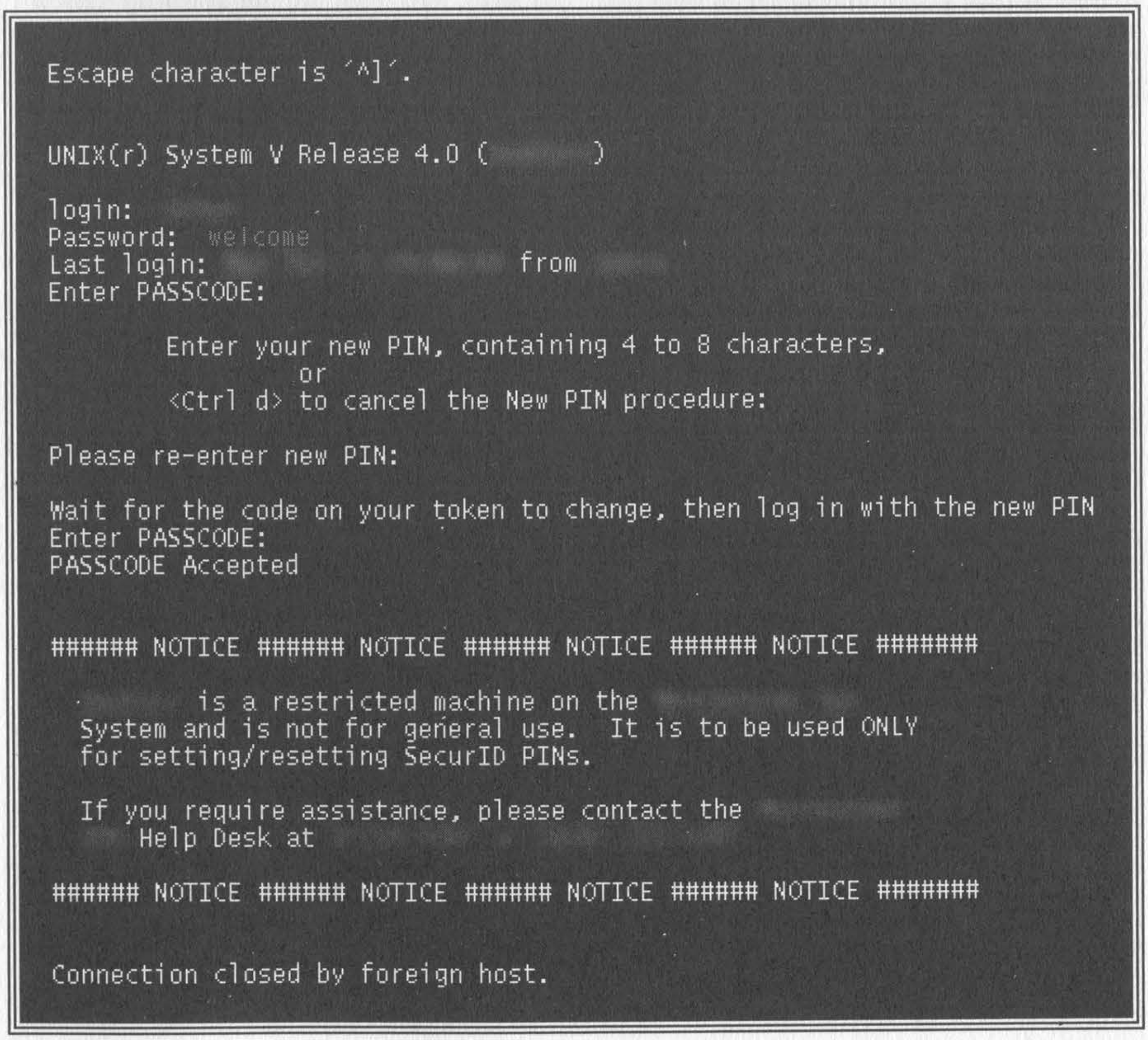
The user enters his or her username (or employee number, or whatever), his PIN and the reading on the SecurID card. The central server knows the serial number of the card issued to this specific user and can look up the random seed. It then runs the SERVER time through the CARD'S random seed. To allow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

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

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

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

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


```
Escape character is '^]'.

UNIX(r) System V Release 4.0 ([redacted])

login: [redacted]
Password: welcome
Last login: [redacted] from [redacted]
Enter PASSCODE:

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

Please re-enter new PIN:

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


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

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

  If you require assistance, please contact the [redacted]
  [redacted] Help Desk at [redacted]

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


Connection closed by foreign host.
```

YOUR INTERNET BIRTHDAY

by The Cheshire Catalyst

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

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

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

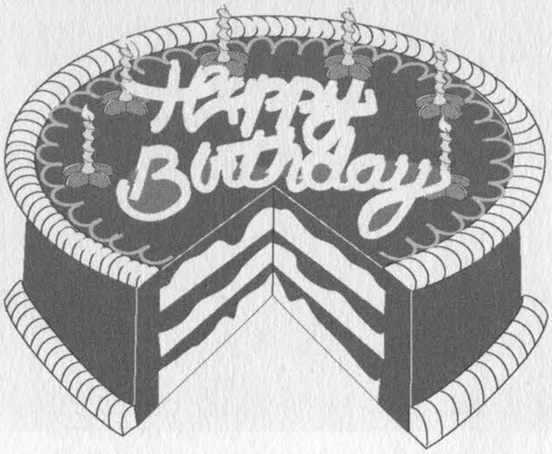
The net is a pretty insecure medium, and three things can pretty much get you into all the trouble anyone wants to get you in. Your name, Social Security number, and date of birth. By using your Internet DOB, someone might have a harder time causing mischief with your identity if they can't find your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

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

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

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

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



Make spammers work for you

By Chatreaux

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

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

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

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

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

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

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

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

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

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

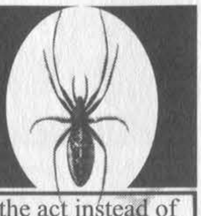
Other kinds of spams carry a URL to invite you to check a web site. These sites will *always* have forms for you to add your information. I suggest you fill them out and also look at the html code of the page with the form. You are likely to fin d a legit email address there.

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

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

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

Taking Advantage of All Advantage.



by silicon kill

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

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

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

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

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

alladvantage.com

AT&T s Gaping Hole

By Jinx

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

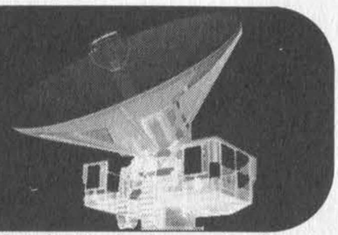
Prepaid activations require specific prepaid numbers from a certain exchange and prefix However, when you activate a prepaid phone with a "regular" cell phone number, what happens is pure magic. A person is able to make and receive as many calls as he wants... for free. You don't have to buy a prepaid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

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

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

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

Cellular Networks Detailed



by EchoMirage
webmaster@echomirage.com

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

The Phones

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

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

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

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

AMPS

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

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

TDMA

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

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

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

TDMA phones use ESNs for tracking.

CDMA

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

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

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

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

GSM

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

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

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

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

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

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

iDEN

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

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

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

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

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

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

WE'RE LISTENING

Alien Intelligence

Dear *2600:*

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

CgK

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

Bookstores

Dear *2600:*

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

Downsouth

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

Dear *2600:*

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

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

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

Anonymous Barnes and Noble Music Seller

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

Dear *2600:*

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

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

quash

Adventures in School

Dear *2600:*

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

Xkalibur

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

Dear *2600:*

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

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

P2129, the student formerly known as Kevin

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

Dear *2600:*

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

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

Of course, next year I have to switch schools, so maybe that one will be worse. Perhaps I too will write an article or letter complaining about my "guilt by association." I hope not.

phil

Dear *2600:*

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

gopher the contradictory

Dear *2600:*

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

Microkiller

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

Discoveries

Dear *2600:*

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

280 open tcp http-mgmt

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

darky0da

Dear *2600:*

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

casey

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

Dear *2600:*

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

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

Handle6015

Dear *2600:*

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

Mongo

Dear *2600:*

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

brain

Dear *2600:*

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

robert

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

Dear *2600:*

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

Dr. K

And with a capital "s" too.

Dear *2600:*

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

carls_pub

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

Kevin Free

Dear *2600:*

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

Koishii

Dear *2600:*

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

KuNg

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

Dear *2600:*

I saw "Free Kevin" all around, but I never really started getting into it until this summer. This school year I have done around ten assignments on Kevin and his situation. We have to do a weekly news topic summary in my Social Studies class and I did a lot on Mitnick while all that really important stuff was happening in September and October. I have also written one or two essays on him. Eventually my class just expected my article to be on Kevin every week, and that's when I realized I actually got the word out. When I found out that Kevin was being released I was overcome with joy. I was jumping and screaming all over the house. This pissed off my parents given it was 3 am on a school night. I also saw that he needs cash for when he gets out. I shall donate soon, we all should. When I read the "hacked" David Letterman top ten list of things to do with Free Kevin stickers, I didn't know how to feel - pissed because he was making fun of the subject, or laughter for it's showing that the message is getting out and being shown in a funny matter. But either way, I'll be sure to watch that episode. When does it air?

Chris from Chrisconsin

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

Dear *2600:*

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

Free Kevin, Free Leonard.

ASZ

Dear *2600:*

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

Rave669

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

Dear *2600:*

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

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

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

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

Dear *2600:*

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

r00t_Canal

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

More on SecurID

Dear *2600:*

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

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

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

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

Kingpin
L0pht Heavy Industries

More Fun in Retail

Dear *2600:*

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

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

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

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

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

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

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

Anguirus

Dear *2600:*

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

The Wedge

Dear *2600:*

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

cashmolia

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

Dear *2600:*

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

MustardMan

Dear *2600:*

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

Phelix

Dear *2600:*

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

cashmolia

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

Dear *2600:*

It has come to our attention that you have published an article, allegedly written by a former employee of Staples. The article itself concedes that it is written by a former disgruntled employee who is volunteering trade secrets and proprietary information of Staples. The clear intent of this article is to encourage malicious destruction of property and stealing. Should you choose to continue to provide assistance to this individual's criminal activities as well as criminal actions by others, you are of course subjecting yourself to liability.

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

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

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

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

Jack A. VanWoerkom
Senior Vice President,
General Counsel
Staples

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

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

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

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

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

Dear *2600:*

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

squatex

Anti-Venom

Dear *2600:*

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

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

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

The Devil

Additional Details

Dear *2600:*

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

netsplit

Dear *2600:*

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

Cilo

Dear *2600:*

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

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

Platinum Dragon

Defeating Corporate Advertising

Dear *2600:*

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

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

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

orn

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

Dear *2600:*

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

Alpha

Help Needed

Dear *2600:*

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

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

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

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

xequals1

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

Dear *2600:*

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

Dan Wheeler
MSNBC Interactive

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

Dear *2600:*

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

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

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

Lubdub

State of the Hacker World

Dear *2600:*

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

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

Pestilent

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

Dear *2600:*

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

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

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

Mind Plague of The Committee

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

Dear *2600:*

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

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

JL

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

Dear *2600:*

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

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

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

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

phiber_life

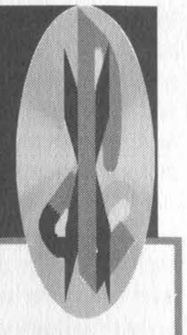
People who show no desire to learn and are only looking for shortcuts deserve sarcasm. Those who are always unwilling to help others are not hackers in the true sense. But then again, neither are those who give up at the first sign of adversity.

Dear *2600:*

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

Continued on page 48

How PSX Copy Protection Works



by Lord Xarph

xarph@blueneptune.com

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

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

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

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

Country Codes

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

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

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

Playstation Model Numbers

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

SCPH-xxx0: Japanese model.
SCPH-xxx1: US/Canadian model.
SCPH-xxx2: PAL/Europe model.

SCPH-100y: This one is the very first Playstation model. It comes in two flavors: below serial number 592000, and above. If you have the lower serial, you can play imports or CDRs without modifications. If you have the upper, you can, but it's so damn hard you shouldn't even try. It came in a box with black sides.

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

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

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

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

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

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

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

Booting Invalid Discs

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

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

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

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

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

Playstation Emulation

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

Legal Ramifications

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

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

> 3.15 - Are CDR backups legal?
>
> In a nutshell: maybe. This is a very confusing topic that has led to many a flame war in the newsgroup. Just so you have some reference points, this is all based off information from the IDSA (International Digital Software Association), the entity you'll most likely be tangling with if you get busted for piracy. The law in question is 17 U.S.C. Section 117(2). As for countries other than the U.S.: If your country has signed the Berne Convention, these apply to you. If not; you're on your own.

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

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

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

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

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

FUN AT CIRCUIT CITY

by ccsucks

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

Price Tags

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

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

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

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

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

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

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

Telephone Fun

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

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

50 PA system on floor and in warehouse

150 PA system in warehouse only (wait for beep)

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

5560 Circuit City Headquarters

5570 FNANB Customer Service

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

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

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

A Little Computer System Glossary

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

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

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

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

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

HOW TO BUILD A COFFEE BOX

by skrooyoo

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

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

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

Materials

You only need three pieces of equipment.

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

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

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

The Voice2000S Mini-Phone

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

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

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

Construction

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

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

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

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

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

Usage

As you would with a beige box, connect it up to your favorite terminals in your favorite local telco box, and have fun.

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

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

Limitations

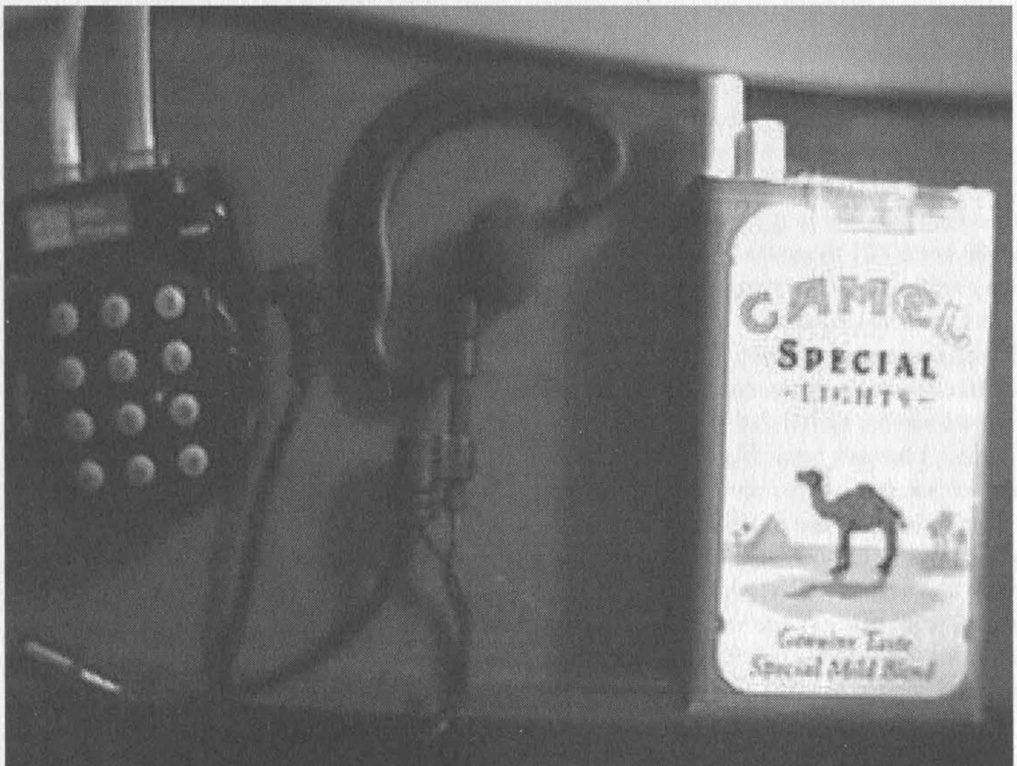
Well, for starters, it has a relatively low Ringer Equivalence Number (REN) of 2.9. What this means is that the total number of phones on any given line should not exceed that number. If you have the Coffee Box attached to two lines (or one line with two other phones), you have an REN of 3 (Coffee +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

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

Credits

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

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



THE SPRINT PCS NETWORK

by ~sn0crash
sn0crash@DigitalPhreak.net

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

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

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

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

ESN - Electronic Serial Number

NAM 1 Phone Number - Your Phone Number

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

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

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

NAM 1 Lockout System - don't know

NAM 1 CDMA Phone Number - your phone number

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

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

NAM 1 Mobile Station ID # - your phone number

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

NAM 1 AMPS Phone Number - your phone number

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

Phone Model - 7 (don't know)

Slot Cycle Index - 2 (don't know)

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

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

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

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

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

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

How to Get Banned From Your Internet Service Provider

by Mandark

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

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

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

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

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

Continued from page 39

blame people like the person above.

Quantum Knight

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

Positive Developments

Dear *2600:*

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

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

ph0x

Idiocy

Dear *2600:*

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

wNdozCRASH

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

Dear *2600:*

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

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

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

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

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

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

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

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

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

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

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

tacit

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

Humor

Dear *2600:*

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

Rick

Big fan of Kevin Spencer and *2600*

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

Forbidden Exchanges

Dear *2600:*

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

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

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

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

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

.244

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

The MPAA Lawsuit

Dear *2600:*

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

Michael F. Nudell

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

Dear *2600:*

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

Punker04

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

Dear *2600:*

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

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

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

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

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

**Anonymous
London**

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

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

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

Dear *2600:*

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

Kevin is *free!*

Apocalyse

Dear *2600:*

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

Wayne

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

Dear *2600:*

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

**Pay_No_Attention_To_That_
Man_Behind_The_Curtain!**

Y2K Issues

Dear *2600:*

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

Desaparecido

Dear *2600:*

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

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

AssMonkey

Dear *2600:*

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

Gustaf

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

Dear *2600:*

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

CubanPete

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

Facts on NT

Dear *2600:*

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

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

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

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

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

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

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

RickDogg

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

Irony

Dear *2600:*

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

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

Knightsabre

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

Free Stuff

Dear *2600:*

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

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

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

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

Twist

Question

Dear *2600:*

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

scorchmonkE

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

2/6/00

Dear *2600:*

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

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

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

Dear *2600:*

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

Rhymezor

DoS Cluebags

Dear *2600:*

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

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

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

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

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

Keith Gardner

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

Dear *2600:*

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

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

Here's hoping....

Andrew

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

Dear *2600:*

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

Cooter

Dear *2600:*

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

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

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

Jason
Louisiana

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

BUILD, DON'T BUY, YOUR NEXT COMPUTER

by bober

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

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

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

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

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

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

Now it's time to talk expansion cards. First, see what's included on your motherboard. Ideally, the only thing there is a keyboard connector, an RS232 serial interface, and a parallel port. You do not want built-in sound, video, and modem connections as are found on most "bargain basement motherboards." As far as a sound card, I would buy one capable of 96KHz and 32 bits, but I am a musician. If you need an explanation of sound compression go to www.mazsound.com for documentation and some good cards for sale. Next comes the video card. Buy a video card with at least 16 and hopefully 32 Mb of ram. You can get away with less but it will, in technical terms, suck.

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

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

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

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

Have fun!

HOW DOES THAT DSS CARD REALLY WORK?

by Phredog

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

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

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

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

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

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

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

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

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

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

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

MARKETPLACE

Happenings

H2K - HOPE 2000 will be taking place on July 14, 15, and 16, 2000 in New York City at the HOtel PEnnsylvania (the site of the first HOPE Conference in 1994). This time we have two floors and enough room to do whatever we want. Start planning now! Reserve your room at the hotel by calling (212) 736-5000 (sentimental types can dial PEnnsylvania 6-5000). Mention that you're with the H2K conference to get the discounted rate. Unlike previous HOPE conferences, we will be running this one around the clock beginning on Friday morning and ending on Sunday night. We expect at least two tracks of speakers as well as music, films, and a/v presentations of all sorts. Registration for H2K is $40 and includes admission to all events throughout the three days. You can send your registration to: H2K, PO Box 848, Middle Island, NY 11953. Make checks or money orders payable to 2600. Be sure to include your name, address, and, if possible, an email address. You can also register online at www.2600.com. If you'd like to volunteer to help at the conference, email volunteers@h2k.net. If you're interested in giving a presentation, email speakers@h2k.net. We also have a mailing list for ongoing discussion about the conference. Email majordomo@2600.com and put "subscribe h2k" on the first line of the mail. Continue to check www.h2k.net for updates.

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

For Sale

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

HTTP://PAOLOS.COM since 1996. Lockpicks, auto entry sets, confidential trade publications, survival tools, an exciting line of affordable switchblades, powerful air rifles and pistols, and a complete line of super-realistic Airsoft guns. *Danger: do not brandish these guns in public, you may be arrested/shot.* We guarantee what we sell UNCONDITIONALLY for 30 days, in addition to factory warranties, and will beat the competition's prices hands down! No "spy store" or "Y2K" hype here, you won't believe it! Visit us to post messages to our discussion board, add your email to our mailing list, or place an order with our easy-to-use catalog! We can ship internationally, and will only sell to qualified customers. U.S. customer can now pay with VISA/MC.

PLAY MP3S IN YOUR CAR OR HOME: Mpjuke unit plays mp3 cd, cdr, and dvd disks. Can be mounted in car, home, or even inside a free drive bay of a PC. It can be trunk mounted in a car or placed under the dash. The unit is self contained, pre-assembled, and it includes a wireless remote. For more information, visit: http://www.mp3carplayer.com/2600 or e-mail 2600@mp3carplayer.com. Sign up for our affiliate program and earn some cash. Resellers needed. $25 from every 2600 sale will go to the Kevin Mitnick fund. We will ship anywhere that we can.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd for hard copy or CD-ROM PDF/GIF version with lots of extra related data and plans for voice changers, scramblers, tone boxes, bugging, etc.) $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

HACKERS WORLD. 650 MB hacking files $15, 650 MB phreaking files $15, Anarchy Cookbook 99 $10, list of warez CDs $5, Surveillance Catalog $5, Virus 99 (730 pages about computer viruses) $5. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

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

HACK THE RADIO: Hobby Broadcasting magazine covers DIY broadcasting of all types: AM, FM, shortwave, TV, and the Internet. It includes how-to articles about equipment, station operation and programming, enforcement, and much more. For a sample, send $3 U.S. ($4 Canada or $5 international). A subscription (4 quarterly issues) is $12 in the U.S. Hobby Broadcasting, PO Box 642, Mont Alto, PA 17237.

PEOPLE WITH ATTITUDE. Check out the political page at the Caravela Books website: communists, anarchists, Klan rallies, ethnic revolt - all at: http://users.aol.com/caravela99 - and a novel "Rage of the Bear" by Bert Byfield about a 15-year-old blonde girl who learns the art of war and becomes a deadly Zen Commando warrior - send $12 (postpaid) to: Caravela Books QH93, 134 Goodburlet Road, Henrietta, NY 14467.

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

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

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $15 (s/h incl.) buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 40A Weis Rd., Albany, NY 12208.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $79.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, PO Box 11562-ST, Clt, Missouri 63105.

Help Wanted

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

NEED HELP WITH CREDIT REPORT. Please respond to B. Mandel, 433 Kingston Ave., P.O. Box 69, Brooklyn, NY 11225.

HELP TO FIND TROJAN HORSE PROGRAM. Understand there is a Trojan Horse program which may be added as an attachment to an e-mail (which appears innocuous when viewed or read) but which will execute and record any password used by the recipient and then send it by e-mail to an outside recipient. Further, that if the outside recipient doesn't receive it for any reason, the e-mail message with password(s) will not bounce back to the sender. Also, there is another Trojan Horse program which, after it installs itself in the UNIX-based ISP of the target, will mail out copies of all incoming/outgoing to an outside recipient without the target being aware of it. Can anyone help with complete information, details, and programs? bryna5@usa.net

I NEED TO OBTAIN credit report information on others from time to time with little or no cost. Can someone help? test/test@usa.net

NEED HELP FINDING AND USING WAREZ SITES. I am looking for several specific graphic, photo, and music production programs. Need help getting to them. Compensation will be given for working full versions. E-mail netvampire@iname.com for list or details.

NEW, COOL WEB AND PRINT MAGAZINE. It will be the Time/Life, People, Spin for generations X, Y, and Z. Looking for writers on all subjects or anything of interest. E-mail jobs@whynotmag.com. Benefits include publication, free stuff, concert and event tix and passes. Photographers and artists also wanted. Join NOW!

TELEPHONE NUMBER HELP. Help to find list of telephone numbers for each telephone company/city where a testman calls to find out all telephone lines connected to a particular address. Also where can one get unlisted telephone numbers without cost. The information used to be somewhere on the Internet. help-discover@usa.net

I AM LOOKING FOR ASSISTANCE in cracking alphanumeric password protected MS Access files. Please send all info to laptop300@yahoo.com. Your help will be greatly appreciated. In return, anyone needing info on WHCA (The White House Communication Agency), I will be happy to lend assistance with copies (or fax) of all ground fiber (T1 through OC128) in DC metropolitan area or other documents.

Wanted

MINIATURE PEN-MICROPHONE that is very sensitive and transmits at least 300 feet to an FM radio. Need the name/address of manufacturer(s) (and prices if available). Reply to b/o/b@usa.net.

I'M LOOKING FOR THE ORIGINAL/OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter.I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at menace26@hotmail.com or icq 13693228. I want the ORIGINAL copies only.

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

Services

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a semantic warrior committed to the liberation of information who specializes in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 986-5591 or (415) 986-5591, at omar@alumni.stanford.org, or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

CHARGED WITH A COMPUTER CRIME in any state or federal court? Contact Dorsey Morrow, Attorney at Law and Certified Information System Security Professional, at (334) 265-6602 or visit at www.dmorrow.com. Extensive computer and legal background. Initial phone conference free.

Announcements

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site. Your feedback is welcome at oth@2600.com.

THE FAMILY, a close-knitted anarchy social group has formed for hackers, phreakers, and computer nerds. Join with your kind in furtherance of independent ideology, financial freedom, and prosperity. Master the possibility of collective thought and association with members of your own mindset. For further enlightenment as to the lifestyle of the family, break the old mold, dare to explore, contact: Purceh Branson, Drawer K, Dallas, PA 18612.

Personal

LOOKING FOR NEW FRIENDS. Am in the Corruption Center of America (Corrections Corporation of America) prison doing a skidbid that's taking too long. Need stimulation and information. Am WM 5'10", brown hair, brown eyes (for the ladies). Used to go as Admkirk on irc. Bored out of my mind and looking to make a connection. Steven Lezak, #000091-A0250176, Diamondback Correctional Facility (CCA), P.O. Box 780, Watonga, OK 73772-0780.

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

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Summer issue: 5/15/00.

MEETINGS

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Sammy's Snack Bar, on the corner of Grenfell & Pulteney Streets. 6 pm.
Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.
Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 6 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Merchant Tea & Coffee (183 Murray Street). Meet outside. 6 pm.
Sydney: Central Station in the main "dome" of the country trains area by the big clock and Burger King. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6pm.
Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Calgary: Eau Claire Market food court (near the "milk wall").
Edmonton: Sidetrack Cafe, 10333 112 Street. 4 pm.

British Columbia

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

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.
Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.
Leeds: Leed City train station outside John Menzies. 6 pm.
London: Trocadero Shopping Center (near Picadilly Circus), lowest level. 7 pm.
Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

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

GREECE

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

INDIA

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

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

MEXICO

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

POLAND

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

RUSSIA

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

SCOTLAND

Aberdeen: Outside St. Nicholas' Church graveyard, near DX Communications' mid-union street store. 7 pm.
Glasgow: Central Station, payphones next to Platform 1. 7pm.

SOUTH AFRICA

Cape Town: At the "Mississippi Detour".
Johannesburg: Sandton food court.

UNITED STATES

Alabama

Auburn: Courtyard outside the computer lab at the Foy Union Building. 7 pm.
Birmingham: Hoover Galleria food court by the payphones next to Wendy's. 7 pm.
Tuscaloosa: University of Alabama, Ferguson Center by the payphones.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.
Tucson: Barnes & Noble, 5130 E. Broadway.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.
Sacramento: Round Table Pizza, 127 K Street.
San Diego: Leucadia's Pizzeria on Regents Road (Vons Shopping Mall).
San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.
San Jose: Orchard Valley Coffee Shop/Net Cafe (Campbell).

Connecticut

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

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Myers: At the cafe in Barnes & Noble.
Miami: Dadeland Mall on the raised seating section in the food court.
Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.
Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Web Site Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 808-922-1677, 808-923-9292.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Ft. Wayne: Glenbrook Mall food court. 6 pm.
Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.

Kansas

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

Kentucky

Louisville: Barnes & Noble at 801 S Hurstbourne Pkwy.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & McDonald's, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: Plantation Coffeehouse, 5555 Canal Blvd. 6 pm.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Michigan

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

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.
Duluth: Barnes & Noble by Cubs. 7 pm.

Mississippi

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

Missouri

St. Louis: Galleria, Highway 40 & Brentwood, elevated section, food court area, by the theaters.
Springfield: Barnes & Noble on Battlefield across from the mall.

Montana

Butte: Butte Plaza Mall on Harrison Ave. near JC Penney and GNC.

Nebraska

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

Nevada

Las Vegas: Wow Superstore Cafe, Sahara & Decatur. 8 pm.
Reno: Meadow Wood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

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

New Mexico

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

New York

Buffalo: Galleria Mall food court.
New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.
Rochester: Marketplace Mall food court. 6 pm.

North Carolina

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

Ohio

Akron: Arabica on W. Market Street, intersection of Hawkins, W. Market, and Exchange.
Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.
Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area.

Oklahoma

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

Oregon

McMinnville: Union Block, 403 NE 3rd St.
Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.
Memphis: Cafe Apocalypse.
Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.
Dallas: Mama's Pizza, Campbell & Preston.
Ft. Worth: North East Mall food court near food court payphones, Loop 820 @ Bedford Euless Rd. 6 pm.
Houston: Galleria 2 food court, under the stairs near the payphones.
San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in the food court.

Vermont

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

Washington

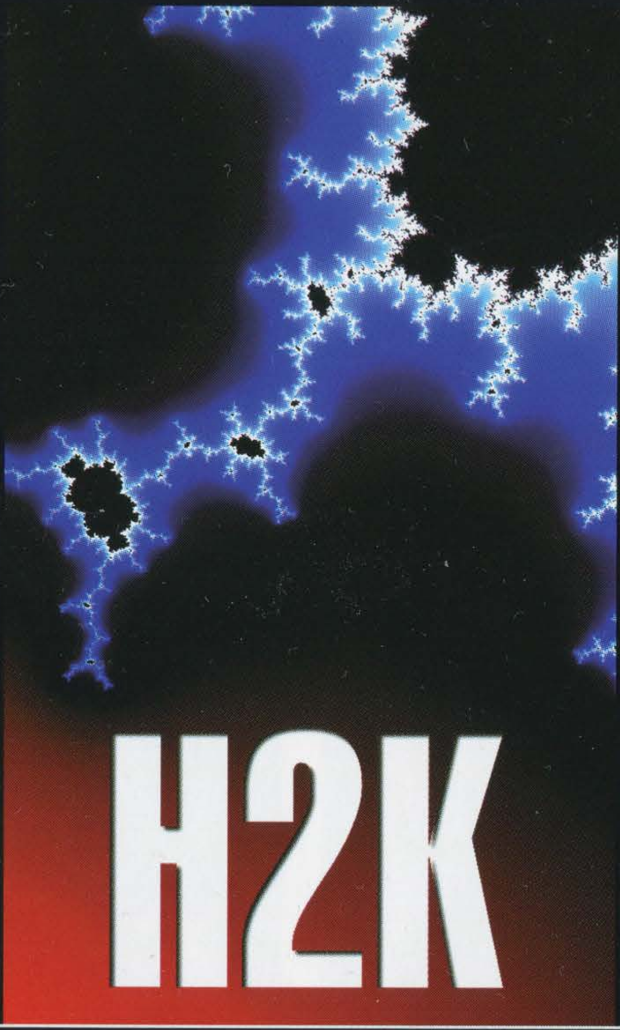
Seattle: Washington State Convention Center, first floor.
Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: London Square Mall food court.
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.
Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (631) 751-2600 or send email to meetings@2600.com.

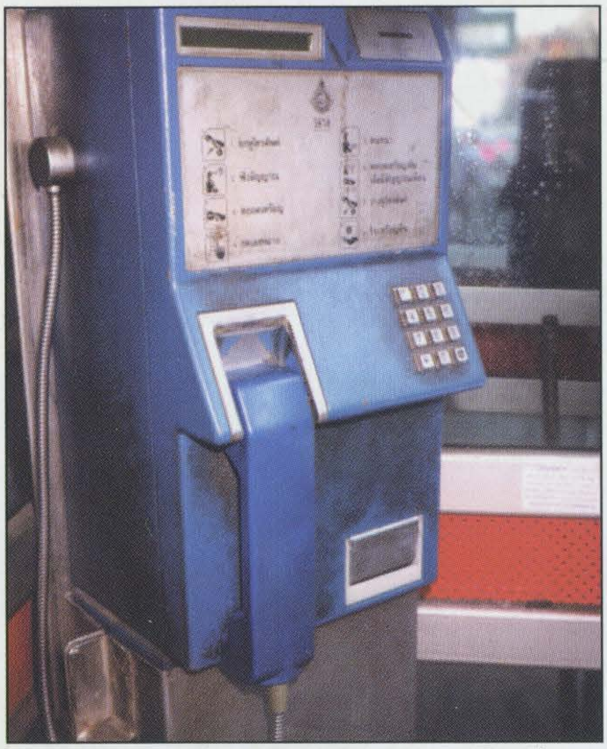
HOPE 2000
HOtel PEnnsylvania
New York City
July 14th to July 16th, 2000



Full details on page 56.
Updates on www.h2k.net.

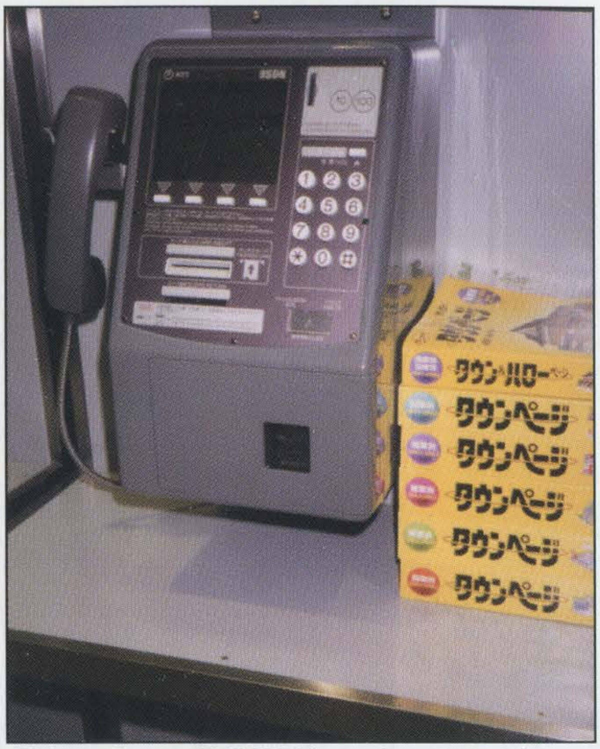
Join us for this historical event!

Asian Payphones



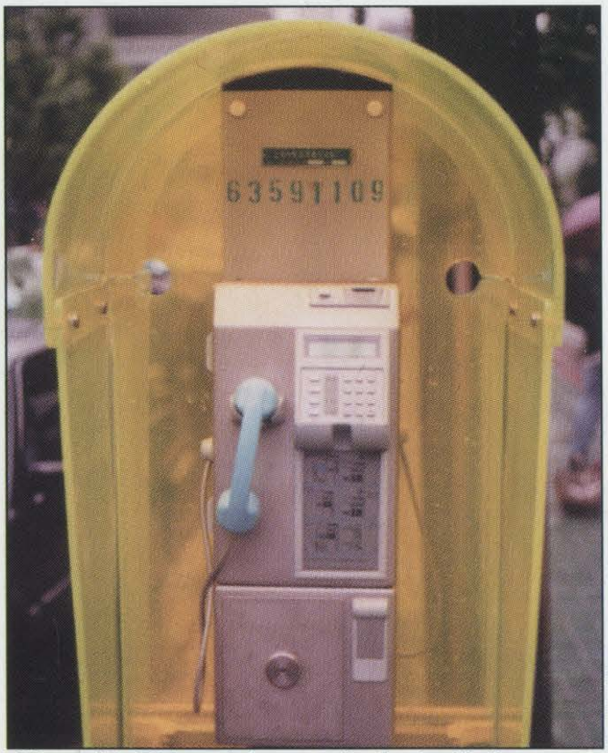
Bangkok, Thailand. This phone looks like it's been through an awful lot.

Photo by MC Telecom



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

Photo by MC Telecom



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

Photo by Julian

Beijing, China
Happy telephone workers.

Photo by Julian

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