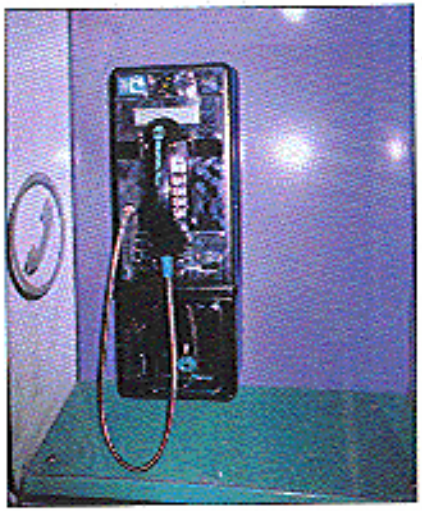
Foreign Payphones

Santiago, Chile. Living proof that a bright red phone always brightens up a street.

Photo by Sol Perez

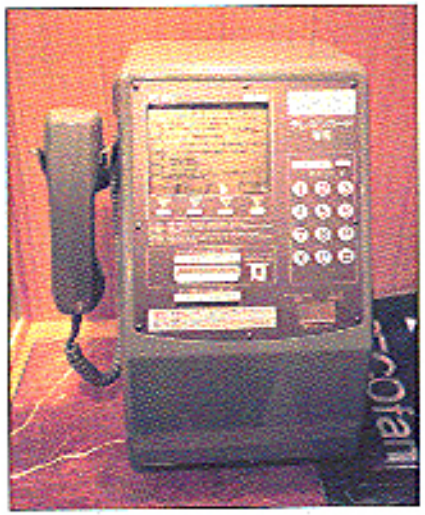


Santiago, Chile. This is what that ugly metallic shine will get you - glare and lots of it.

Photo by Sol Perez

Athens, Greece. Found at the base of the Parthenon.

Photo by Peter Photopoulos



Kyoto, Japan. An ISDN phone that looks too intelligent for its own good. We wouldn't be surprised if it speaks.

Photo by eclip5e

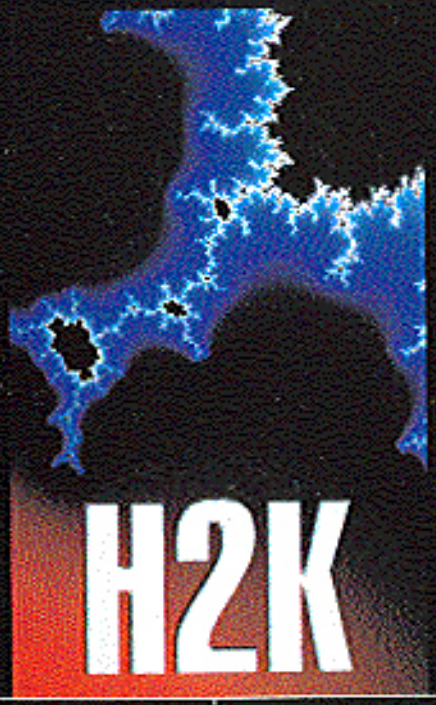
Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

Volume Sixteen, Number Four
Winter 1999-1900
$5.00 US, $7.15 CAN

2600

The Hacker Quarterly

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



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

Join us for this historical event!

WHAT REALLY MATTERS

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

STAFF

Editor-In-Chief
Emmanuel Goldstein

Layout and Design
ShapeSHIFTER

Cover Design
sinc, The Chopping Block Inc.

Office Manager
Tampruf

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

Webmasters: Kerry, Mackl

Network Operations: CSS, Izaac

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

IRC Admins: autojack, russ

Inspirational Music: Joe Strummer, Syd Barrett, real early Floyd, Ron Geesin

Shout Outs: Hippies From Hell, etoy, claudus, t12, The Stony Brook Press, www.indymedia.org, Studio X, and everyone who stood up in Seattle

RIP: Krystalla

Good Luck: Naftali

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

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

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

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

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com).
2600 Office Line: 516-751-2600
2600 FAX Line: 516-474-2677

Violence, Vandals, Victims

As the 90's fade into history, it's not likely the unhealthy trends of our society will do the same anytime soon. In many ways we've become practically enslaved to the corporate agenda, to the great detriment of the individual.

The signs have been around for a while. You've seen them repeatedly in these pages. People interested in technology who ask too many questions or probe too deeply or thoroughly are seen as a threat because they might adversely affect profits or embarrass those in authority. The net has steadily been transforming from a place where freedom of speech is paramount to one where it all revolves around the needs of business.

Now there's nothing wrong with commerce, people making a profit, or even people who just don't care about the things others value. After all, there's room for all types in the world as well as on the net. But that's not how it's panning out. Increasingly, the needs of the individual are being sacrificed for the needs of big business. Corporate mentality is replacing our sense of individual liberty. And it's pointing us down a very dark road.

Consider things that have happened in the very recent past.

A teenage hacker from Washington State pleaded guilty to hacking several prominent government web sites, including the White House and the United States Information Agency. Despite there being no damage caused to any of the sites (apart from embarrassment and having the index.html file renamed), the government felt that 15 months in prison and a $40,000 fine was appropriate. Reports say he *could have gotten* 15 years and a $250,000 fine.

Later that same month, coincidentally in the same state, police fired tear gas and shot rubber bullets at a crowd of peaceful demonstrators who were protesting the World Trade Organization's meeting in Seattle. Many said it was the worst civil unrest since Vietnam.

At first glance, you might not think these stories have very much to do with one another. But when you analyze them a little more closely, it's not difficult to see that they are both symptoms of the same disease.

Much of the unprovoked brutality inflicted by the Seattle Police went unreported, despite the abundance of sound and picture images. But every major network dutifully ran a story about the "violent anarchists" who started all the trouble. In the end, whenever the word "violence" was mentioned, one thought only of those people.

Zyklon caused no damage to any of the systems he got into. Yet the mass media painted him as someone dangerous. He renamed a file. But all reports say that he shut down the USIA for eight days. This is how long it took them to install decent security, something they had never bothered to do in the first place. He didn't take away their security - they never had it to begin with. But this fact wasn't seen as relevant in any of the stories that ran. And what about the act of taking a young person away from his friends and family for more than a year and forcing him to live with potentially dangerous criminals? Well... *that's* justice.

In both cases that which is most precious to our society - the individual - was made to suffer because their actions and form of expression caused humiliation of some greater power. We've seen this before in the hacker world with Bernie S. and Kevin Mitnick (who is at last scheduled for release on January 21, 2000). People who go to forbidden places, utter forbidden speech, or are just seen as an inconvenience are stepped on, abused, even tortured.

Why punish such relatively harmless individuals, whether they be hackers or demonstrators, with such passionate vengeance? Could it be that their very existence constitutes a real threat that the authorities have no idea how to handle?

In Seattle, the disparities between what happened and what was reported were almost comical - vandalism of commercial property being reported as violence whereas violence against individuals was mostly glossed over, with the exception of certain foreign and alternative media. What kind of a society are we turning into when commercial losses are more important than the human injuries? How could the good people of Time/Warner (CNN) have missed this? Or Microsoft and General Electric (MSNBC)? Or even Disney (ABC)? Why would such bastions of journalism ignore the real story? Were they maybe more concerned with whether the WTO would continue to look out for them and their interests?

We may indeed have developed a horribly cynical outlook on society. It's hard not to when things like this are so often tolerated. But the flipside is that our view of the individual has only strengthened. If there's one thing we've learned from recent events, it's that people aren't as brain dead as we were led to believe. People *do* care, they are paying attention, and they see the ominous tones of the future. Few persons seem to trust the government anymore, big business is increasingly seen as a threat to our freedom, and individual troublemakers are filling our expanding prison system.

It's not very difficult to see how we got to this sorry state. All of the mergers and consolidation of power have carried a heavy and inevitable price. The real question is how do we regain control of our destinies?

Continued on Page 55

Accessing Forbidden NTFS Drives

by NumberSyx

The following information is described for the purposes of education. I'm aware this procedure could be and has been used to circumvent the security of any Windows NT machine which the user has physical access to. I do not condone the use of this information for illegal purposes, nor am I responsible for anything stupid anyone does with this information. NTFS support in Linux is still Beta, reading and copying from the drive is safe, but copying to the drive is an "at your own risk" deal.

Intro

One of the many misconceptions about Windows NT is that it's a secure operating system and that by formatting a disk with NTFS and properly setting permissions, nobody can access the information on that disk without permission to do so.

There are two problems with this theory. First, it is *wrong*. Second, all it really does is make crash recovery more difficult. I will describe a method for circumventing NTFS security: using a Linux boot disk. This can be useful in many ways. From the system administrator's view, this is an excellent way to get access to important files on a system that has crashed before formatting the hard drive and reinstalling NT. From the hacker's view, it gives access to the system files. He would not normally have access to the registry, user profiles, PST Files, etc.

In order to accomplish this you will need some knowledge of Linux. It is possible to do this with a DOS bootable floppy, but the only NTFS drivers available are read only and therefore useless to me. In all fairness, Linux has this vulnerability as well.

The first thing you need is a copy of the latest version of Trinux. This is a Linux mini distribution designed for network administration and it has many useful features. Its best feature though is its ability to boot from a floppy on virtually any machine which has more than 8 MB of RAM.

Get two blank floppy disks, go to www.trinux.org, and download the following files: boot.gz, classic.gz, ntfs.o, and rawrite.exe. The current version as of this writing is 0.62, however use version 0.61 as there is not enough room for extra files on the 0.62 boot disk. Follow the instructions for unzipping and making the boot disk and the data disk. If you can't get this far, you have no business doing this in the first place.

When this is done, copy ntfs.o to the boot disk, edit the Modules file, add the line "ntfs" to it (no quotes), and save the file. At this point it is best if you boot the disk a few times, first to test it and second to get familiar with what will happen and how Trinux will respond to commands given it. This way there are no surprises.

What Next

Now take the two floppies to the machine you want to access. Boot the first disk. When it asks if you have a data disk, put in the second disk and type "y" then hit return. It will then ask you again. Type "n" and hit return.

When it is finished booting, you will have a "Trinux 0.61" prompt. Type "insmod ntfs.o" - this loads the NTFS support.

Type "mount -t ntfs /dev/hda1 /mnt" - this will mount the first partition on the first hard drive. This assumes the first partition on the first hard drive is an NTFS partition. If not, the following table will give you an idea of how to mount the proper drive.

These are for IDE drives:

/dev/hda1

/dev/hda2 second partition on the first drive

/dev/hdb1 first partition on the second hard drive

/dev/hdb2 second partition on the second hard drive

You get the idea. Now you should have access to the drive. You can now put a third floppy in the drive and type "mount -t msdos /dev/fd0 /floppy". This gives you access to the floppy so you have someplace to save files to. Alternately, if you are really clever you could get the proper modules for zip drive support which connects to the LPT port (scsi.o and pps.o), which would give you more flexibility in copying files.

I would like to give creative credit to CM, who challenged me to find a way to access an NTFS system from a floppy disk.

Security Through NT? Not Likely

by Kurruppt2k

For quite some time, hacking has meant knowing a decent amount about UNIX, or, for you old-school hackers, VMS, TSO, or whatever. Maybe you would have to know a tad about Netware, but that was as far into the PC world as you cared to delve. Well, it's 2000 now, and Microsoft is getting its foot into the World Wide Web, meaning the percentage of NT machines on the net is increasing. A lot. Now, many of you UNIX-only hackers refuse to even glance in the direction of a Windows box, but NT is only going to get bigger as time goes on, not to mention Windows 2000 (active directory... ooh!). And what if the web page you want to deface happens to be sitting on an NT Server? You're just going to have to suck it in and learn to break into NT machines too.

My least favorite thing about Windows is its poor socket capabilities. This means less open ports when you scan, which means less daemons to play with, which means less points-of-entry. And if you search the exploit archives for NT stuff, you won't find much besides DoS sploits and stuff that needs to be executed locally on the NT LAN. All of a sudden your ocean of UNIX hacking techniques is about 10 percent applicable in the NT world.

For starters, NT is an NOS, meaning a client/server environment. If you telnet to a UNIX machine and execute a command, your request is processed on that machine, using its resources. If you connect to a Windows box and issue a command, the process is launched onto your computer, using your resources, and if it's a command that reports system information, it gives you info on your own computer. How do you execute commands to be run on your target Windows machine? Suddenly those NT machines seem untouchable. Not true.

How to hack an NT box all depends on what exactly your goal is. With UNIX, you're usually looking to get a root shell. As I'm sure you know, you can't have a "shell" on a remote NT box. NT is set up to share resources - files, applications, printers, you get the idea. Meaning each workstation in its network exists as an entity in itself (vs. dumb terminals logging into a huge UNIX machine), and if it needs something from a server, you have to connect to it via NetBIOS. In Windows Networking, this means mapping a logical network drive to a particular share.

Microsoft Networking

Shares. The heart of Windows networks. A share is just like a volume in Netware - a directory setup to be accessed from authorized persons/workstations inside the network/internetwork. Shares can either use share-level security, or user-level security. Share level security means that the resource is protected by a single password, and anyone knowing that password can access the share. User level security is more UNIXish, in that your permissions to a particular share depend on who you are logged in as. Now, this entire article refers to breaking into NT over the Internet, so logging in isn't feasible (though it is possible, see the "Elite Tactics" below). If port 139 is open though (which it almost always is on an NT Server, and oftentimes is on NT Workstation and Windows 9.x), you can use Client for Microsoft Networks to connect to it.

First make sure you have the client installed - go to Control Panel, then Network (you should also have NetBIOS, NetBEUI, and TCP/IP installed). You will use the Net command to do this. Once you find your target NT machine and see an open port 139, your first step is to find out if there are any open shares. To find out, type this at a command prompt:

C:\net view \\[ip address]

If you get no error message, it probably means that the computer you attempted to connect to had no open shares (or possibly that you don't have Windows Networking set up correctly on your machine, so check!). If shares exist, you will see a list of them, including the share name, share type (disk, printer, etc.), and any comments the sysadmin wanted to mention. For more NetBIOS infor-

mation on this machine, use the "nbtstat" command. If you see no open shares, there is still a possibility of hidden shares. Common hidden share names include:

* (samba)
*SMB (samba)
*SMBSERVER (samba)
ADMIN$ (remote administration - can you say "root shell"?)

To connect to any share, visible or hidden, you again use the Net command, in the following fashion:

C:\net use i: \\ip address\[share name]

To check for hidden shares, just try to connect to the names given above, or any others you can think of. If it exists, you'll connect. Once you receive the "The command was completed successfully" message, you are connected to the NT machine. Logical drive I: (or whatever drive letter you assigned) now becomes that share - you've mapped a network drive to it. This is similar to mounting remote filesystems in UNIX. So to see what you've connected to, change to drive I: and issue a "dir". You can now use any DOS commands to explore the share. The share, however, may be password protected. You may be prompted for a password right after issuing a Net Use, or after connecting when trying to browse the filesystem. Typical hacker methods can be used to defeat this. If, however, you get a message that you do not have privileges to that resource (or "access denied"), this means that the share is user-level, and since you can't really log on, you won't be able to access the share. Once in, you will have either "read" permissions, meaning you can look at or execute (launch into your RAM) a file, or "read/write," meaning you can edit any file as well. To check, make a file and delete it. Create a directory and delete it.

Utilities

Here I will outline a few useful tools you should have when planning to break into an NT box.

Legion is a Windows sharescanner - it will automate doing Net View commands on an entire subnet (or multiple subnets). Launch it, sit back, and watch as it combs networks for open shares. If you prefer doing everything from UNIX, WinHack Gold will do the same thing.

NAT (Network Auditing Tool) is a great program by the makers of Legion. It will attempt to connect to any open share you specify, attacking with passwords you provide in a wordlist. It also looks for hidden shares.

L0phtCrack is an NT password cracker. Getting NT passwords can be tricky - see the "Password Cracking" section.

And finally, **AGENT SMITH.** This program will essentially brute force the hell out of your target, and log all responses to a file of your choice. Oftentimes this will be your only way to break through password protection on your share.

All four of these program are available at The CyberUnderground (www.users.uswest.net/~kurrupt2k).

Password Cracking

All the hashes reside in the SAM (Security Account Manager) hive of the registry. To get the hive, you have a few options. If you're running Windows NT yourself, you can install L0phtCrack and attempt a Remote Registry Dump. If the machine you're targeting allows for registry sharing, you will have the entire SAM hive imported into L0pht. More often, though, this doesn't work. You could always do a core dump, convert the output into ASCII, and pick out the hashes. But that can be time consuming and messy (not to mention you'd have to upload software to perform a core dump). So you may have to resort to going after the SAM hive stored on the hard disk of the machine (or any other Domain Controller on the network). The file you are looking for is "sam._". The problem is that NT hides this file from users and essentially disables it from being accessed while NT is running. To get it, you'll have to boot the computer to an alternate OS (Linux, DOS, etc.) and get it that way. Another problem is that the hive is on an NTFS partition. DOS, of course, uses FAT, and Linux uses EXT2, so you'll need a program to access the alien partition (such as NTFSDOS). Installing another OS onto the remote machine will most likely be tough, as will forcing it to reboot, though programs exist that will do it. If nothing else, try DoSing it to force it into rebooting. So before you devise a vile plan to put DOS 6.22 and dosreboot.exe onto your target, and change the boot.ini, look around for backup copies of sam._. It's not unheard of to find an old copy in something like "C:\winnt\pdc\repair".

Also, if you prefer to crack passwords with UNIX, you'll have to convert the hive to a UNIX passwd file (cut and paste the hashes).

FTP

The closest thing a hacker can do to telnetting in to an NT machine is connecting via FTP. The problem is that just because an account exists on the machine doesn't mean that it's allowed FTP access. So get the password hashes, crack them, and try to FTP into them all.

If the sysadmin thinks he's smart, he'll rename the Administrator (root) account. Either way, if you crack the password, you'll have FTP access with administrative privileges. You can now deface web pages, get more passwords for other computers on the network, upload trojans, etc. Here's a trick: copy the Event Viewer program to a shared directory, then Net View to it. You now have access to all logs on that machine.

Elite Tactics

Okay, let's pretend you have FTP access. The problem is, you can't execute programs or do anything else that's any fun. The answer - a trojan. Get one that allows you complete filesystem access, allows for screenshots of your target computer, and lets you open and kill active windows (NetBus does all of this). But how do you run the trojan once you upload it? You have a few options. Put it in the autoexec.bat or autoexec.nt file, and force it into rebooting (possibly with a DoS attack), or just wait until someone reboots it. Another ploy, if the machine is a web server: upload the trojan into a CGI directory (cgi-win, cgi-dos, cgi-shl, etc.), then request the trojan with a browser. If you state the path correctly, the web service will spawn (launch) the trojan for you. Now just connect with your client, and you have complete control of the computer.

Here's another scenario. Let's say you want to hack their web page. You have a few passwords, but the FTP service has been disabled. Well, if the web pages reside in a share (unlikely) you can use MS-DOS EDIT to edit the default.htm or index.html file. Otherwise, you can always use HTTP to upload your file. Netscape and Internet Explorer both have clients to upload html files via HTTP - just use the user names and passwords you cracked.

Network sniffers can also be put into place. L0phtCrack comes with SMB Packet Capture, a decent sniffer. Search the net for other NT, Ethernet, or Token Ring sniffers. The point here is that if there is even one Windows 9.x machine on the network, it sends cleartext (ASCII) passwords when authenticating, so a sniffer will always catch them.

There are also a huge variety of exploits for NT. The trick is weeding through the DoS spoits and the local ones. One remote exploit, iishack.exe/iishack.asm (www.eeye.com) theoretically will upload any file (in your case, a trojan) right through IIS's HTTP daemon. IIS ships with most NT Server packages, and comes with one of the earlier service packs. Even if the machine in question isn't a web server, it probably has IIS installed. One popular web server for NT is WebSite Pro, which has a vulnerability in its packaged CGI executables. Specifically, uploader.exe allows you to upload files to the computer - without passwords.

Now, when I said that you can't log on to an NT Server over the Internet, that was partially wrong. The only way to log into an NT network is to be a member of the domain. So you'll have to make your computer a member. How? Hack the PDC (Primary Domain Controller) or a BDC (Backup Domain Controller). Now, chances are if you've gotten far enough "in" to make yourself a member of the domain, you probably have all the permissions you could ever want. If not, launch the program called User Manager for Domains and add yourself, with your IP address.

In Summary

All in all, NT is a very different environment than UNIX or VMS. It also demands very different skills and techniques to hack. Doing so is just as rewarding as breaking into a SPARC station, and will provide you with all kinds of new and useful information. This is, after all, why we do what we do.

Countermeasures Revisited

by Seuss

The most prevalent information on telephone counter-surveillance has been floating around for at least 15 years. Short the pair at the demark and measure resistance. Open the pair at the demark and measure the resistance. Abnormally high or low resistances indicate a phone tap. Forrest Ranger wrote about it in text files, M.L. Shannon and Paul Brookes included it in their books, and an untold number of phone phreaks have employed this technique. Despite its popularity, the technique has its shortcomings: it fails to detect devices installed in the outside plant, split pairs are undetected, and transmitters built into the phone are not tested for.

What you'll need:

1) Access to a local DATU.

2) A multimeter with high impedance scales (several meters that measure into the giga-ohm range are available) and a capacitance meter.

3) An induction probe.

4) A frequency counter or near field detector.

5) Something that makes continuous noise, like a tape player.

6) Ancillary tools (screwdrivers, a can wrench, etc.).

First, call the phone company to ask about your line's readiness for ISDN or DSL. High-speed services demand a line with no loading coils and a minimum amount (less than 2500 ft.) of bridged taps. Either will cause inaccurate measurements.

Begin by taking the phone off hook and turning on your tape player (to turn on voice activated transmitters). Now give your phone a pass with your near field detector or frequency counter. Transmitters in the phone will hopefully be picked up at this point. (Note: some speakerphones are prone to normal RF leakage.) Next, measure the capacitance of the line, dividing the value by .83 (the average mutual capacitance for a mile of phone line). This is roughly the length of your line. Write it down, you'll need it later. Remember that .83 is an average value, which can range from .76 to .90 depending on line conditions. To get a more accurate measurement you can fine tune your figure by comparing capacitance measurements on a section of plant cable of a known length, or use a TDR.

Disconnect all the phones from the line you want to test. Go to your demark and disconnect your pair on the customer access side. Short the pair and measure the resistance of the line from the farthest jack with the meter set to its lowest scale. Reverse the polarity of the meter and measure again. If either resistance is more than a few ohms, it would suggest a series device wired into the line somewhere on your property. Now return to your demark, open the pair, and cover the ends in electrical tape. Measure the resistance of the pair with the meter set to its highest scale. A less than infinite resistance would suggest a device wired in parallel to your line.

Testing in the outside plant should be conducted from the teleo side of the demark point in order to avoid measurement error from the station protector circuit. Call that DATU and short the pair, then measure the resistance of the line. Compare the value you got for your line's length with the figures below:

Note: 5ESS switches incorporate a "test bus" that will add about 500 ohms to the shorted pair.

These figures will vary with temperature, splices, wet sections, and a host of other reasons. Large deviations could (but don't necessarily) suggest something wired in series with the line. This measurement may be supplemented by either a resistance to ground measurement of both sides of the pair and a capacitance balance test or a voltage measurement. A resistive imbalance of more than 10 ohms or a noticeable drop in off-hook voltage calls for further inspection.

To test for parallel devices in the outside plant, open the line with the DATU and repeat the parallel test as described above.

Wire Gauge	Loaded Pair	Unloaded Pair
26ga	84.33	83.33
24ga	52.89	51.89
22ga	33.72	32.39
19ga	17.43	16.10

Testing for telephone hook-switch compromises requires an induction probe. Reconnect your pair at the demark and plug all your phones back in. Turn your tape player back on and put it near your phone. Now probe all the lines coming through your demark point. If you hear the tape player through the probe, your phone's hook-switch has been compromised.

Checking for splits on your line requires an induction probe and access to a plant wiring cabinet. Add a tone to either lead of your pair with the DATU. Probe all the conductors in the binder pair, listening for the trace tone. If you hear the tone on more than two leads (the ones connected to the line you're checking) your line has been split. This can be either a bad splicing job, or someone intentionally hooking a pair up to your line.

If any of the above tests suggests that there is something on your line, remember that there are plenty of innocent reasons a test could turn up positive, so a detailed physical search is in order. Disassembling the phone in question and comparing the innards to a schematic would be a wise idea at this point. Take the covers off your phone jacks, dig around in your demark point, peek inside wiring cabinets if you can, and so on. There are some places that are likely out of your reach, but keep in mind that they're likely out of reach to many wiretappers as well.

DATUS - The Tool of the New Age Phreak

by MMX

Most of this article is adapted/condensed from the administration manual. But be honest with yourself before criticizing me for "stealing" this article. When was the last time you called Harris and SE'd it out of them? Huh? Didn't think so bitch.

The Harris Direct Access Test Unit Remote Terminal extends the field technician's testing capabilities of subscriber lines through the non-metallic environment of a pair gain system. Typical pair gain systems include SLC 96, SLC-Series 5, etc. The system has three major components: the Direct Access Test Unit (DATU), the Pair Gain Applique II (PGA II), and the remotely located Metallic Access Unit (MAU).

Direct Access Test Unit - Remote Terminal

The DATU-RT is a printed circuit card that provides microprocessor control of line preparation functions, voice prompted menus, and status reports to the technician. It allows technicians to access and perform specific loop conditioning and tone generating functions on any working subscriber line to prepare the line for use with field test equipment. The card is installed in the Metallic Facility Terminal (MFT) bay and connected to the Central Office switch.

Pair Gain Applique II

The PGA II is a printed circuit card that extends the DATU-RT capabilities into the pair gain environment and serves as the interface between the DATU-RT and the switch's Pair Gain Test Controller (PGTC). It determines the status of the PGTC and its metallic DC test pair, provides carrier channel signaling and transmission test results, and controls the DATU-RT's access to the MAU. The card is installed in the MFT frame and connected to the switch.

Metallic Access Unit

The MAU provides the standard DATU-RT line conditioning functions as directed by the DATU-RT. It eliminates the need for metallic bypass pairs from the switch to the remotely located pair gain terminal. The enclosure is installed inside the cabinet housing the pair gain equipment. One DATU-RT and one PGA II, working together in the same switch, may serve a maximum of 212 separate MAU locations. The RT system provides the technicians the ability to perform a series of line preparation functions to subscriber lines. These functions are established and maintained by authorized personnel.

Now, onto my part of the article.

I won't be speaking about administrator mode for three reasons:

1) If you accidentally screw something up, the DATU probably won't work.

2) You don't own any DATU that you're using (nor do you have permission), and therefore you're committing a crime by accessing one.

3) I think that if I talk about things like changing the NTT Busy Test, you will do something naughty. Very naughty.

However, I will consider releasing an article on DATU Administrator functions in the future.

To access the DATU, dial the telephone number assigned to it. Upon connection, you will hear a 440hz "dial tone" indicating that the DATU has answered and is ready for password entry. Dial the password of the DATU, which is defaulted for technicians at 1111. If the first digit of the password is not entered within seven seconds after the DATU answers, it will release the line. Upon entering a successful password, another DATU dial tone is heard, prompting you to dial the seven digit subscriber line number (in other words, the number you want to test). Occasionally, something will be wrong at the CO, the DATU will say "Error, had no test trunk" and a pulsating 440hz tone will be heard. If you ever get this, then you probably are accessing a DATU either at a CO where someone is asleep at their desk or in a remote office. I have yet to get this error at a heavily manned CO. You also won't be able to run tests if you get this message.

After the DATU prompts you to dial the subscriber line number, a few things can happen. If you dialed a number not served by that DATU, you will get the message: "INVALID PREFIX" and another DATU dial tone. Upon dialing a correct number, if the line is idle, the DATU accesses the line and you will hear "Connected to ddd dddd. OK. Audio Monitor." You can then select a line conditioning function anytime after the voice message begins, including the ten seconds of audio monitor before the menu is presented. If the line is busy, the DATU will say "Connected to ddd dddd. Busy line. Audio Monitor." The busy line will then be monitored for 10 seconds. It should be said at this point that all audio traffic is unintelligible. After the ten seconds of audio monitor, the DATU will send two 61-Hz tones in rapid succession to indicate the end of the monitor period. Features that would be disruptive to a call in progress are not available if the DATU-RT detects a busy line condition. These functions include "High-level Tone," "Open Subscriber Line," and "Short Subscriber Line."

There are theories about confusing the DATU by changing its busy test in administrator mode. Theoretically, if you change the busy test on the NTT, you could say, open your ex girlfriend's line while she was on the net cyber fucking her new boyfriend.

DIAL 2 FOR AUDIO MONITOR.
DIAL 33 FOR TIP/RING SHORT TO GROUND.
DIAL 37 FOR RING GROUND.
DIAL 38 FOR TIP GROUND.
DIAL 44 FOR TIP/RING HIGH LEVEL TONE.
DIAL 47 FOR RING HIGH LEVEL TONE.
DIAL 48 FOR TIP HIGH LEVEL TONE.
DIAL 5 FOR LOW-LEVEL TONE.
DIAL 6 TO OPEN SUBSCRIBER LINE.
DIAL 7 TO SHORT SUBSCRIBER LINE.
DIAL STAR TO KEEP TEST AFTER DISCONNECT.
DIAL POUND FOR NEW SUBSCRIBER LINE.

Functions of the DATU

Anyway, after learning the status of the line, the functions are presented in a menu format. Main Menu functions are announced as follows:

Most of these functions actually aren't as exciting as they sound, *if you're on crack*. A quick description of each of the functions:

1 - Announce Main Menu.

2 - Audio Monitor. Provides a way to verify that the busy test was correct. Traffic on the line is audible but unintelligible. Audio Monitor is automatically disabled at regular intervals to insure that the DATU-RT is able to detect DTMF tones in the event an exceptionally strong audio signal is present. This occurs at regular six-second intervals and is of approximately two seconds duration.

3 - Short to Ground. The "Short to Ground" function is used to connect the Tip, Ring, or both leads to Ground potential. If only a single lead (Tip or Ring) is selected, the opposite lead is unterminated.

4 - High Level Tone. This function places 577hz high-level (+22 dBm) interrupted tone bursts on the Tip lead, Ring lead, or both. If a single lead is selected, the opposite lead is grounded. This function is typically used for the purpose of conductor or pair identification.

5 - Low Level Tone. This function places 577hz low-level (-12 dBm) interrupted tone bursts on both the Tip and Ring leads. Because the tone signal is longitudinal, use of this function does not disrupt traffic on a busy line. Tone bursts can be heard only on a telephone instrument connected between Tip or Ring and Ground. This function is typically used for the purpose of conductor or pair identification on a busy subscriber line.

6 - Open Subscriber Line. The "Open Subscriber Line" function removes Battery and Ground potentials from the subscriber's Tip and Ring leads.

7 - Short Subscriber Line. The "Short Subscriber Line" function provides an electrical short across the subscriber's Tip and Ring leads.

** - Hold Functions (Keep Test After Disconnect).* The "Hold Test" feature provides a means by which a line condition asserted by the DATU-RT is maintained for a specified time interval after disconnecting from the DATU-RT. The duration of the Hold Test interval is entered through the telephone keypad and is specified in minutes. Any interval may be entered; however, the DATU-RT will not maintain a line condition longer than the Access Timeout interval. The programmed function is automatically canceled by the DATU-RT when the specified time interval or, if of a shorter duration, the Access

Timeout interval has elapsed. (At this point, it should be noted that upon setting up a DATU, the administrator determines the Access Timeout Interval, which is basically a timer to say "good-bye" once you've lounged too long on the DATU. By default, the Access Timeout is 10 minutes. Also, after hitting *, the DATU will prompt you with either "DIAL NUMBER OF MINUTES" or "DIAL 2 DIGITS FOR NUMBER OF MINUTES." With respect to single digit entries, "0" is interpreted as 10 minutes. Also, after you use this function, the DATU will expect you to be finished and will say "PLEASE HANG UP.")

8 - New Subscriber Line. This function releases the currently held subscriber line so that another subscriber line may be accessed.

Before moving on, there is one other function that is worth mentioning.

9 - Permanent Signal Release. The "Permanent Signal Release" function causes the removal of Battery and Ground potentials from a permanent signal line served by a step-by-step switch. This function is typically used to clear a busy condition resulting from a line fault so that normal line tests may be performed. After pressing "9" on the keypad, the DATU responds with "PERMANENT SIGNAL RELEASE." After executing the required sequence of operations, the DATU tests the subscriber line to determine whether the busy condition has been cleared. The result of this test is then announced as either "OK" if the line is idle or "BUSY LINE" if the line is busy. This function is not available unless specifically enabled by the DATU administrator. Unless enabled, any attempt to use this function results in the message "ERROR - PERMANENT SIGNAL RELEASE DISABLED." Permanent Signal Release will function only on a line that the DATU has identified as busy. An attempt to use this function on an idle line results in the message "ERROR - IDLE LINE."

Single Line Access

You may be saying at this point, "Gee, MMX, how do you find the measure of the interior angles of a regular polygon?" If you're saying this, you probably are on a large number of prescription drugs. Moving right along... If you should find yourself "testing" the line that you're calling the DATU with, you will realize that you can't test that line, since you're using it to call the DATU. An interesting predicament. The DATU is prepared as always to handle your problem. By dialing "*#" before the subscriber line number, the DATU will wait until you hang up, and then test the line. Pretty simple, eh? Oh yes, and for those who wonder why there is no "audio monitor" during single line access after you select the test function, the DATU will ask you for the "number of minutes." The testing doesn't start until one minute after you hang up.

Sadly, the actual Administrator's Guide won't go into great detail on the use of each feature of the DATU more than three times by the end of it. Stupid corporate products.

Conditioning of Carrier System Lines

Note: Unless you have a fairly basic grasp of the way pair gain systems operate, I would suggest skipping this section.

After dialing the subscriber line number, if the line is on a pair gain system, the DATU announces, "ACCESSING" and repeats the subscriber telephone number entered. The DATU announces the state of the subscriber line/NTT with one of the following voice messages:

"PAIR GAIN LINE, PROCESSING" - if the line is idle and is a pair gain line.

"BUSY LINE" - if the line is busy.

If the selected line is busy, the DATU cannot determine whether the line is served by a carrier system. It is, therefore, not possible for the DATU to activate the Pair Gain Test Controller (PGTC) and metallically connect the DC Bypass pair at the RT to the subscriber line. Without this metallic connection, the DATU cannot condition the line. In this case, only the "Audio Monitor" and "Low-Level Tone" functions are available to the user. Because its signal is longitudinal, the Low Level Tone function is generally not effective when used on a busy carrier system line. If the line is idle, the DATU attempts to activate the Pair Gain Test Controller (PGTC). The PGTC, in turn, tests the carrier channel and communicates the results to the DATU. These operations require additional time and may result in a delay of up to 30 seconds. After successfully completing these steps, the RT system identifies the carrier channel as follows:

"SINGLE-PARTY LINE" - if a single party channel unit is detected.

"MULTI-PARTY LINE" - if a multi-party channel unit is detected.

"COIN LINE" - if a coin channel unit is detected.

If the DATU is unable to activate the PGTC or the PGTC encounters a problem in testing the carrier channel, the DATU issues one of the following voice messages:

"BYPASS PAIR BUSY OR PGTC FAILURE" - the DC Bypass pair is in use, all PGTC test circuits are busy or the PGTC cannot complete carrier system connections.

"PAIR GAIN SYSTEM ALARM" - the carrier system serving the selected line is in a major alarm condition.

"CHANNEL NOT AVAILABLE" - channel test results were not provided by the PGTC.

"BAD CHANNEL" - channel tests failed - possible bad channel unit.

After a failure in carrier channel tests or in activating the PGTC, the DATU remains in Menu Item Selection mode so that the central office personnel may more easily determine the problem. If one of the above error messages is heard, however, the DATU is probably not connected to the line to be tested. Therefore, line conditioning commands will be accepted and confirmed by the DATU but the condition may not necessarily exist on the line anytime after one of the above error messages is heard.

Remote Terminal (RT) Access

After the DATU has successfully accessed the subscriber line and acquired channel test results, the DATU will say "PLEASE ENTER PAIR GAIN SYSTEM ID, DIAL STAR TO END." Enter Pair Gain System ID using telephone keypad. To condition line from Central Office using the bypass pair, enter "0*". Use the following section (Alphanumeric Pair Gain System ID Entry) if Pair Gain System ID includes alphabetic or punctuation characters. If selected, the bypass pair must be in place between the host element of the DATU at the Central Office and the RT.

Alphanumeric Pair Gain System ID Entry

This section describes the method by which alphabetical letters may be entered using a standard 12-key DTMF keypad.

a. Enter any leading numbers that are part of the Pair Gain System ID in the normal manner.

b. Enter "#*". This key sequence places the RT system in a special mode in which alpha and certain other non-numeric characters may be entered as a series of two-digit key codes.

c. The first key depression simply identifies the key on which the desired character is stamped or printed. Press the key on which the character appears. For example, if character is "A", "B", or "C", press the "2" key.

d. The second key depression identifies a single character from the group (typically three letters) selected with the first keystroke. The character is identified by its position on the key. To select the first, press "1". If the desired letter is the second of the three, press "2". Press "3" if the desired letter is the third of the group.

e. Repeat steps c and d for each alpha character in the Pair Gain System ID. When the last character has been entered, enter "*#" just as previously done in step b. This restores the "numeric entry" mode. Special two-key sequences are assigned to the letters "Q", "Z", and certain punctuation characters. Table 1 below outlines these.

f. Enter any trailing numbers that are part of the Pair Gain System ID.

g. Any combination of letters and numbers may be entered in this manner. Repeat the appropriate steps as necessary.

h. Enter a single star (*) to complete the Pair Gain System ID entry.

i. After the Pair Gain System ID has been successfully entered, the DATU will say "PLEASE ENTER PAIR NUMBER. DIAL STAR TO END." Enter the pair number for the subscriber's line using the telephone keypad.

j. The DATU provides verification of the Pair Gain System ID entry with a voice message. If a valid ID was entered, the DATU announces "ACCESS" followed by the ID previously entered. If the Pair Gain System ID is

not valid or if the bypass pair was selected, the DATU announces "USE BYPASS PAIR."

Two-Key Sequences-Non-Numeric Keypad

1st Key \ 2nd Key	1	2	3	4	5
1	(space)	.	-	'	/
2	A	B	C		
3	D	E	F		
4	G	H	I		
5	J	K	L		
6	M	N	O		
7	P	R	S	Q	
8	T	U	V		
9	W	X	Y	Z	

Some Words About Male Voiced DATUs

At this point, I should mention (at least something) about those DATUs with an incredibly sexy male voice. These are an extreme rarity at the date of writing. In fact, in a list of over 200 DATUs that I have, I only know of one that still works. Upon speaking to the man at Harris who actually developed the DATU, he said, "It's so old, you could blow dust off it." However, since it is still in use, I will soon be writing some words about it. Please note that if you find a DATU I in use, I would love to get a recording of the administrator menu for it.

Last Remarks (for this issue)

To begin my ending, I would like to say to anyone who thinks "Hey, cool, I'll DATU an AOL access number and make it busy," is not only lame and stupid, but also factually wrong. The NTT can't access burnt lines, and you may inadvertently set off an audible alarm at your CO by doing so. Oh yes, and the "LO SURVE" LED of the DATU will go on when you try. In the future, I will go into the wild and crazy world of the test interface for non standard offices. Following that, well, I'll see what I can dig up for you. Perhaps something about (dare I say) - Administrator mode?

Physical and Electrical Specifications

(directly copied from administration manual)

Physical

Dimensions

Length: 8.0 inches
Width: 7.5 inches
Height: 2.0 inches
Weight: 1.7 pounds

Electrical

Battery Input Requirement (measured with respect to CO ground)

* -46 to -54 volts DC
* 600 mA maximum
* 2 volts peak-to-peak noise maximum from CO

Access Line Interface (Ground Start)

1. Tip and Ring Parameters in Off Hook Mode

* Meets FCC Part 68 requirements
* Resistance is 130 - 280 ohms at 20 to 80 mA
* Minimum DC current required is 20 mA
* Typical AC impedance, at 1 kHz, is 640 ohms

2. Tip and Ring Parameters in On Hook Mode

* Meets FCC Part 68 requirements
* Minimum ring detect level is 65 volts AC rms
* Uninterrupted pre-trip ring duration is 300 ms
* Ringer equivalence is 0.5B

3. Secondary Dial Tone

* Secondary dial tone is provided upon ring trip, password entry, and new subscriber line selection
* Dial tone is silenced when a digit is dialed or when the DATU-RT times out
* Dial tone level is -16 dBm +/-3 dBm
* Dial tone frequency is 440 Hz +/-8 Hz
* Harmonic distortion is less than 10%

4. DTMF Dial Decoding:

* Each incoming dual-tone signal is translated into one of the 12 character sets shown in Table 2
* Frequency deviations of up to +/-2.5% are accepted and all deviations greater than +/-3.5% are rejected
* DTMF tones greater than 50 ms are accepted
* Interdigit timing is greater than 40 ms and less than seven seconds are accepted
* Signal strength per frequency of -20 to 0 dBm are accepted

5. Voice Message Output

* Average voice level is -19 dBm
* Voice frequency range is 200 to 3,000 Hz

No Test Trunk Interface

1. Tip and Ring Parameters in Idle Mode

* Resistance is greater than 20M ohms

2. Tip and Ring Parameters in Active Mode

* Resistance is 100 to 180 ohms at 20 - 90 mA
* Maximum DC current is 90 mA
* Typical AC impedance, at 1 kHz, is 660 ohms

3. MF Output Parameters

* Each outgoing dual-tone sinusoidal signal is translated from one of the 12 character sets shown in Table 2
* Frequency deviation is less than +/-2%
* Signal strength per frequency is -5 to -15 dBm
* Digit duration is 70 ms
* Interdigital pause is 70 ms

4. Dial Pulse Addressing Parameters

* Percent break is 60%
* Repetition rate is 10 pulses per second
* Interdigital time is 1,000 ms

5. Sleeve Current Parameters

* Low current mode is 7 to 10 mA into 120 ohm sleeve
* High current mode is 50 to 70 mA into 120 ohm sleeve
* Maximum external sleeve loop resistance is 700 ohms

Test Function Parameters

1. Open test is greater than 20M ohms

2. Tip and ring shorted is less than 2 ohms

3. Tone Test

* Frequency is 577 Hz
* Frequency error is less than +/-3%

4. Low-Level Tone Test

* Typical signal strength, measured tip-to-ground or ring-to-ground:
* At the CO is -12 dBm +/-3 dBm
* At 18,000 cable feet from the CO is -19 dBm

5. High Level Tone Test (Differential)

* Tip to-ring signal strength is +22 dBm +/-3 dBm
* Tip-to-ground or ring-to-ground signal strength is +17 dBm +/-3 dBm.

Acronyms That You Are Too Stupid To Know

DATU - Direct Access Test Unit
HILARY - Guess!
PGA - Pair Gain Applique
PGTC - Pair Gain Test Controller
RT - Remote Terminal

DTMF and MF Decoding

Frequency Groups / Character	DTMF Low	DTMF High	MF Low	MF High
1	697	1209	700	900
2 (ABC)	697	1336	700	1100
3 (DEF)	697	1477	900	1100
4 (GHI)	770	1209	700	1300
5 (JKL)	770	1336	900	1300
6 (MNO)	770	1477	1100	1300
7 (PRS)	852	1209	700	1500
8 (TUV)	852	1336	900	1500
9 (WXY)	852	1477	1100	1500
*	941	1209		
0	941	1336	1300	1500
#	941	1477		
ST			1100	1700
KP			1500	1700

MESSING WITH STAPLES

by Maverick(212)

Well, as you might guess, I used to work for Staples, The Office Superstore. Used to, that is, until they fired me over something which was, even for them, ridiculous. So, here I am, spilling my guts about the technology used in their stores.

Phones

The stores use a standard Meridian phone system with six lines: the first three outgoing local and the last three special lines. These special lines are only good for 800 calls and calls to other stores and cannot be used for regular local and/or long distance calls.

To dial another store, either hit one of the regular line buttons and dial the regular phone number, or, from any of the lines, dial the store's 700 number. Each store has two 700 numbers, one for voice and the other for fax. The voice lines are always 1-700-444-xxxx, where xxxx is the 4-digit store number, padded with initial zero's, if needed. The fax lines are always 1-700-555-xxxx. As far as I know, these 700 numbers are only good when calling from inside a store.

Sometimes, the outgoing lines require a password. This is not too common, but is easily circumvented. By punching FEATURE'' from any phone, you can access the phone system's configuration menus. It does ask for a login and password but the defaults are invariably 266344 ("CONFIG"). The only phone line in the stores that will work in a power outage is the one the fax machine at the copy center is plugged into.

The phones also feature, in the lower right corner, a "page" button. "May I have your attention, Staples shoppers...."

Ribbon Computer

Located next to the selection of typewriter and printer ribbons in every Staples store is an old 386 computer that is constantly running a program which is supposed to assist customers in finding the proper ribbon. This standalone system has no security whatsoever. Simply pressing the spacebar to kick off the screen saver and hitting Ctrl-Break is enough to drop you to a DOS prompt. (Rebooting and breaking out of the autoexec.bat is also trivially possible.) Unfortunately, once you are at a DOS prompt, there is really nothing much to do, as all the ribbon-finder files are in a special format. One thing that is possible is changing the screen saver image. It's located at c:\ribnfndr\scrnsvr2.pcx, and is a standard 640x480 pcx file.

Proteva

Staples sells custom-built Proteva computers. These are displayed and sold through a stand-alone system at one end of the computer wall. The "kiosk" simply allows customers to look at specs, select various system packages and options, and print out a price quote. This system runs Windows NT, and is susceptible to the ntisdos trick. (Booting from a floppy and running the shareware program ntisdos allows read-only access to the hard drive.) Copying the Sam file and running it through L0phtCrack reveals five different users and passwords. The Administrator password is at least somewhat secure - a full two weeks running L0phtCrack didn't reveal it. The other logins/passwords are:

"Guest" - this account is disabled.

"customer":none - this account is used for regular customer browsing.

"update":"STAPLES1234" - this one automatically loads new features/pricing from a diskette.

"mis":"STAPLES1234" - this allows you to change the current pricing and make an update diskette which can be loaded on the same or other machine using account "update".

Compaq BTO

Staples also sells Compaq Built-To-Order computers. These are viewed and ordered from a Compaq computer, which is usually placed right next to the Proteva. Unlike the Proteva, however, the Compaq "kiosk" has a power-up BIOS password and is networked into Staples' corporate WAN. This is necessary because the kiosk is only used as a viewer for Compaq's web site where the specs, option lists, and ordering forms really are. The site is available at www.compaq.com/retail. Login and passwords are "STAPxxxx", where xxxx is the 4-digit store code, padded with initial 0's as needed. There is very little security on this computer. Simply pressing Ctrl-Alt-Del, and "End Task"-ing the kiosk software (really Microsoft Internet Explorer run full-screen without the toolbars, etc.) drops you directly to Win95. A new browser can be fired up and whoosh, you can surf the net. Or you can go into Network Neighborhood and look around a little. What else is on the local network? Read on....

Office Computers

Years ago, all each Staples store had in the way of computers was an AS400 terminal. This ran over a 9600 leased line to the corporate headquarters and was used for inventory control, printing price signs, entering damages, and many other tasks. About two years ago, Staples installed Frame Relay T1s to all its stores and upgraded to three actual computers in each store. The Sales Manager's office received a computer, as did the General Manager's. The third was set up as a training computer for employee use, usually in the larger of the two offices. These were generally 266 to 333Mhz Pentiums with either 32 or 64 megs of memory. All ran Win NT 4.0 SP3.

The computer in the Sales Manager's office was usually kept running a terminal program that simulated the AS400 terminal that had been removed. The General Manager's computer was used for making employee schedules and keeping track of employee punches at the timeclock. It was also used every Sunday to do employees' payroll. The training computer was loaded with various certification and educational software and kept track of which employees had passed which "courses" at "Staples U." All three computers had browsers and could surf Staples Intranet and the Internet.

Using ntisdos and L0phtcrack on these machines revealed the following accounts:

Administrator:"018SuWN.9" - Thought they'd make it more secure using a period. Heh heh.

Guest: - Disabled.

InstallNT:"InstallMe" - Used, obviously, for maintenance and installation.

StaplesService:"scivreSselpatS" - Yes, the login backwards.

Associate:"SELL" - What we were supposed to do.

Manager:"CARE" - What the managers didn't.

Sales:"SPLS" - Our stock symbol.

userid:"PASSWORD" - Yes, this account actually exists. Someone must have taken the instructions a little too literally when asked to type in their userid and password.

The Gun

With the arrival of the office computers, Staples stores also received a remote terminal hooked up into the system. This "gun" has a small lcd screen, an alphanumeric keypad and a scanning laser. Almost any function you can do from the AS400 terminal is available from the gun, including price checks, sign printing, and inventory functions.

Security Personnel

Most Staples stores have a security guard at the front door. He (it's usually a he) is the one who asks you to leave your bag with him when you enter the store. He's basically powerless to do anything, though. If pushed hard enough, and backed by a store manager, he can refuse you entry to the store if you refuse to leave your bags with him. But most of the time, he'll let you in with a "I'll have to check your bag when you leave." Of course, you don't have to let him, and he can't make you.

Security Procedures

Staples policy is that a manager can only stop a suspected shoplifter at the door if that manager has kept the suspect in sight at all times from the moment they take something and hide it to the moment they try to walk out the door. This is very difficult, if not impossible, especially if the manager is following the suspect - the manager has to run past the suspect to get to the door first in order to stop him, but can't take his eyes off him. This rule is often ignored, however, as managers sometimes take the word of the security guard, or even the associates as to what has happened. Many times, nothing is done to the suspect, as there is no proof and inadequate surveillance.

Staples has a special code word to indicate a security problem. This code is "Fred Klein," who used to be the head of Loss Prevention for Staples many years ago. By simply paging "Fred Klein to aisle 4," any associate can indicate that there is a suspicious person in that aisle. All other associates are supposed to drop what they are doing and converge on that location en masse in, basically, an attempt to scare the suspect into leaving.

Security Devices

Certain Staples stores, usually those with the highest losses, have gotten a security system installed. It consists of a set of "gates" set on either side of the entrance and exit doors, and rolls of stickers which are placed on high-ticket items. The stickers interrupt the weak magnetic field put out by the gates which causes the gates to beep. This can obviously be defeated easily by removing the stickers from the merchandise.

Some stores also have cameras, usually aimed at the main entrance, and possibly one in the money room.

Well, that's enough for now. When I dig up some more information, I'll be sure to write another article. Until then - happy hacking!

I Own Your Car!

by Shtan

I work the night shift for a major auto company near the motor city in Michigan. One night all the bosses went home early and left us there alone. We had learned earlier that day (on the news) that a bunch of us were being laid off and the rest were being transferred or strong-armed into quitting. The executives didn't even have the decency to tell us first, or in person. We had to hear it on TV. So needless to say, no one was in a good mood.

Where I work there is no getting out. If you quit you have to take 30 days (unemployment) before you can work at another related facility. The software we use is only used by other related facilities. Still they wouldn't release us from our contracts. Most of us had put in years of service and worked overtime to get projects out to match deadlines set by executives who had no idea of the work involved. Even forsaking our families at times, and for what? To be walked on and thrown out like yesterday's newspapers, to perfect a vehicle that we will never be able to afford? No perks at this job, poor pay, no employee discount, no job security, and the night shift makes getting anything done impossible. Basically, they own us.

After learning of our imminent doom, everyone was sitting around wondering what would become of us. Three of us - who were as close to model employees as you could get - did our jobs and didn't screw around while other people slacked off and played solitary. We never took advantage of our jobs. That is, until that one night.

I was the first who mentioned a scheme, half jokingly and half seriously. "We should go down into that restricted area and try to get in." The other two guys agreed we really didn't have anything to lose. So we decided to go for it. We knew what was in there because you could see all the experimental cars from the solid glass walls. The sliding doors were about 10 feet high and 15 feet wide. The only problem was that they were locked by an executive level passkey card. We knew they wouldn't let us walk right in - none of us fit the description of an executive type. We were obvious computer geeks, as our coworkers would say. So we thought of a plan. We gathered a bunch of door parts, a frame here, a sealing strip there, got some calculators, sketch pads, pencils, and a few compasses left over from the manual days. We picked up some heavy blueprints to back up our story and typed up a fake work order. Our pass cards would let us in most of the way but when we got to the glass wall, we were stuck. Sliding my card through, it just beeped. I thought about spraying some salt water in the reader, like what people did in the old days with Coke machines, but that would have been destructive and nonproductive. Instead, social engineering would be our key.

A voice spoke from the intercom. "Can I help you?"

I replied, "The reader won't read my card."

The voice came back, "You're not in the computer for this area."

"I have a job that requires my unescorted access to this area".

"I'll be right down," the voice shot back.

We showed him our ID badges that proved we worked there and he asked what we were doing. We explained that we needed to get in the restricted area to do some last minute changes to the seals in one of the vehicles before this year's auto show, which was only a few weeks away. Unconvinced, the guard wouldn't let us through. We unrolled the blue prints and showed him where the trouble was. Being the senior he was, he couldn't read the blueprints or make heads or tails of it. "There is an airflow problem throughout the door system, which at high speeds causes wind deviation thus amplifying cabin noise and increasing internal pressure." We threw in some more technical BS and buzz words and finally he was convinced after we showed him the phony work order. He slipped his passkey through the door and opened it for us. He watched us for about a half hour until he got a buzz from another part of the building and had to go. We told him this will take us most of the night and we could let ourselves out. There were push-buttons on this side. Now the fun would begin.

Most of you won't see the vehicle we were about to play with until 2002. It's a prototype and there were six of them there. In the trunk was a fuel cell, holding about 50 gallons of racing fuel. The tires of the car were kicked out and set out about 6" in the rear, and mostly to the corners of the car. It was super charged, none of that cheap turbo charge crap. Under the hood was, well you wouldn't believe me if I told you. Needless to say this wasn't the fuel economizing car that everyone thinks we're all working on to save the environment. This car was pure evil. Oh, did I mention that we are one of the most prestigious car companies, that we are the definition of luxury and class? Most older folks want one of our cars when they retire. So this car will be a shock when it's released. And it will be released.

We drooled enough. Now it was time to test out our made-up theory. There are always keys in these vehicles and full tanks of gas. No emblems on the car so no one will know what it is if they see it. Heck, at 2 am who would be out on the roads anyway? We fired her up and two of us went out, leaving one behind to open the door so we could get back in. I took the second spin at the wheel and, oh my gosh, talk about power and speed. I had never driven a super charger before. There was no waiting for the turbo to kick in. You hit the gas and it was pure power. The tires would squeal as long as you held the gas down. At 80 mph it seemed like we were crawling and every time I tapped the peddle the tires would squeal. At 95 mph they would squeal! I think I got whiplash that day. At a red light a Corvette pulled up next to us, a new sleek one. He gunned his engine and when the light changed I floored the gas. Bad mistake - the car just sat there spinning its wheels like we were on ice. OK, I'm a computer geek, not a drag racer. I came off the entrance ramp to I-75 at 75 mph. I was looking for a certain switch that I had heard existed. I flipped off the headlights and hit the switch. Night Vision.

A camera is mounted in the hood in the symbol. It displays the image on the window and you can see through fog and rain. It makes everything white and is very cool. I like it because I can drive with no headlights on. The ride was smooth, and steering was tight and effortless even at speeds over 150. The car also has GPS installed in case you get lost or you lock your keys in it - or if the car is stolen. If you get in an accident and the airbag goes off, it autodials the headquarters and patches you into a 24 hour receptionist who can listen in on your cabin and talk directly to you using cellular towers. This system and features are commonly referred to as telemetry, another new buzzword that will be popping up later this year. The home base of this is networked and the receptionist can watch your car's movement on her screen. She can patch her screen to other receptionists too. Other features of this system allow you to navigate and even be told histories of the towns that you're driving through. No per-minute fees, just one yearly fee. Had I not been having so much fun I would have thought to get the dial-in number to the automated computer.

It was nearing our lunch time so I hit the blue button which connected the car to the 24 hour lady. She gave us her name and asked how she could help us. I said we needed the location of a 24 hour restaurant. She gave us a few of them and then told me to turn right at the next exit and guided me there no problem. All without even asking my name, or where I was calling from. I later learned this service will cost about $400 a year but that is unlimited service calling. Data travels at a slow analog speed of 2400 bps. This should change soon as more digital towers are put up along the expressways. Then all vehicles will use spread-spectrum.

The lady said she was getting a reading of engine compartment heat and suggested I ensure the radiator was full, even though it appeared full to her. It might have been due to my driving over 100 mph for so long before I called her. "I'll check it out," I told her. Just think what other people could do if this fell into the wrong hands. This service makes the Pentium III ID feature look like small potatoes.

Hacking in the future will soon find its way into the automobile. This car itself is one large computer; there are microchips in every part of the car, each controlling components, mirrors, windows, seats, door locks, power brakes, etc. Viruses will be easily inserted into the car's onboard system via the CD player which will soon be a

direct link to the car's CPU. A hacker could make the horn honk every time the brake pedal is pressed. Just think what a program like Back Orifice could do on one of these cars.

I see it like this: A voice announces to the irritated driver: "What's wrong - you don't like Rob Zombie?" *"No!"* yells back the executive driver. "Fine, turn it off. Oh that's right, you can't. *I own your car!!!"*

Most of the top automakers are secretly making it their goal to turn their luxury cars into a virtual onboard LAN. And it was highly evident in the car I was driving. Behind closed doors, execs discuss their future plans. They want their vehicles to be able to access the Internet. It would have to be wireless and they know what that means. A high price would have to be paid to the companies that own the rights to the specific radio spectrum which would be required by this system. They figure they will pass the cost to the consumer and have them pay for the service like we do now for the Internet. (Mental note, invest in AT&T stock.) With all the talk of what they want to do, no one is talking about what they're going to do to make it secure. They are relying on digital spread spectrum to be their firewall saying that will protect them from their signals being intercepted. In my opinion this is very near-sighted, yet typical. What they don't realize is that sometimes the demon comes from within.

I've seen the future, and it is sweet.

```
*** -
*** - Welcome to irc.2600.net - Message of the Day
*** -
*** - IRC - 2600 STYLE
*** -
*** - We all know IRC is an anarchic way of communicating, to say the least.
*** - This is all fine and good, except that it sometimes makes
*** - communicating a bit difficult. A bunch of us have put our heads
*** - together and come up with something that should please everyone - the
*** - 2600 IRC Network. That's right, a new network that's completely
*** - independent of EFNet, Undernet, Galnet, whatever. Simply change your
*** - server to irc.2600.net and you're in!
*** -
*** - As this is our own server, we can do whatever we damn well please on
*** - it and you have more of a chance of implementing features that you
*** - want as well. At the moment, we allow usernames of up to 32 characters
*** - instead of the current limit of 9. We're working on implementing
*** - secure connections for our users so the monitoring agencies can go
*** - back to real crime once again. And, at long last, 2600 readers will be
*** - able to contact people in their areas by simply entering a channel
*** - that identifies their state or country. For example, #ka2600 is the
*** - 2600 channel for Kansas. #2600de is the 2600 channel for Germany.
*** - (States come before the 2600, countries come after. A full list of the
*** - two-letter codes is available on our server.) And, as always #2600
*** - will exist as the general 2600 channel, open to everyone at all times.
*** - You can create your own channels and run them as you see fit, in the
*** - tradition of IRC.
*** -
*** - We look forward to seeing this network grow and flourish. Help spread
*** - the word - irc.2600.net - a network for hackers, run by hackers.
```


Telco-Babble

by Android

The etymological origin of the word telecommunications is derived from the Greek word tele as defined in the book of Webster as to travel a distance over. And communication defined as a system for sending and receiving messages, as by telephone, telegraph, radio, etc. Now that we have an understanding of the concept, let us proceed into the subject and shed some light on it.

This is inspired with respect to our brethren Catatonic Dismay who wrote "Copper Pair Color Coding" in 15:4. I was enlightened to read the article so that others reading about what was written can understand the information in their quest for knowledge in the Information Age. What was explained was the color code. The color code is the foundation to understanding the wires that are used for our telephone connections. When you see a telephone cable, it will be a dull silver/greyish color and will have a variety of different colors of wires. When you strip the wire, it is copper. And of course, copper is a conductor of electricity.

All of the wires have different specified colors with respect to the color code. Understanding the sequence will help you understand how to connect it to a 66 block, for example. Encountering other types of cable with the wires inside will show the various colors of the wires. It will be in a different sequence, but the concept applies as it does to all other telephony cable. Now that there is clarity to the purpose for the wire, I'll expand on the different types of terminology pertaining to how the cable is defined.

For the standard telephony cable, inside there are 25 pairs of color-coded wires. The definition for the 25 pairs of wires is called a binder. From the definition of a binder, we can expand our telco jargon. One super-binder has 25 binders with 625 pairs. One mega-binder is equivalent to 25 super-binders. And last, one ultra-binder has 25 mega-binders or 39,625 pairs of colored wires. This is equivalent to one ultra-fiber optic cable. That wasn't too hard now... was it? What I forgot to add was that for telephony cable, when there are more than several binders, there are ribbons inside to separate each individual binder. What is interesting about it is that the color code applies to it - colors with respect to the color code separating the wires so that no confusion will arise (or did I add to the confusion?). Anyway, this is the definition for the different classifications of wires.

That was the foundation for understanding the various telephony cable sequences with respect to the color code. Practice using the terminology with a telco person who works out in the field and that person will be impressed. As for understanding the various networking protocols, packet-switching, TCP/IP, to name a few, they rarely understand it (not to castigate their intelligence). This is from my social engineering with others in the field. In contrast, the telcos provide us with services that are vital to the connections to the communications terminals so that we can have our Internet and telephone connections.

As a techo-dweeb dilettante, the telco realm was different compared to the computer/electronics realm; two completely different entities. I rarely use the color code, but it's good to share the knowledge with others not familiar with it. When the two are integrated there is an appreciation for the cabling, terminals, and connections making it possible for communication lines to be in existence. Yet, it's fascinating to ponder how a copper wire with plastic wrapped around it in various colors is vital to the communications that we are using today and for tomorrow.

An Intro to Paging Networks and POCSAG/FLEX interception

by Black Axe

Pagers are very, very common nowadays. Coverage is widespread and cheap, and the technology is accepted by most. Ever wonder, though, what happens on these paging networks? Ever wonder what kind of traffic comes across those pager frequencies? Ever listen to your scanner on a pager frequency in frustration, hearing the data stream across that you just can't interpret? Want to tap your radio, get a decoding program, and see what you've been missing?

Before I begin, let's cover just exactly how those precious few digits make it from the caller's keypad to the display of the pager in question. Or perhaps your monitor....

Let's entertain a hypothetical situation in which I would like to speak with my friend, Dave. First, I pick up my phone and dial Dave's pager number (555-1234). I hear the message "type in your phone number and hit the pound sign." So I comply, enter 555-4321# and then hang up.

Here's where the fun starts. This is all dependent on the coverage area of the pager. The paging company receives the page when I enter it, and looks up the capcode of the pager it is to be sent to. A capcode is somewhat akin to an ESN on a cellphone; it identifies each specific pager on a given frequency. The paging company will then send the data up to a satellite (usually), where it is rebroadcast to all towers that serve that particular paging network. (Remember last year, when everyone's pagers stopped working for a few days? It was just such a satellite that went out of orbit.) The paging towers then transmit the page in all locations that Dave's pager is serviceable in. In this case, let's say that Dave's pager has a coverage area that consists of a chunk of the East Coast, going from Boston down to Washington DC, and out to Philadelphia. The page intended for him is transmitted all throughout that region. Since a pager is a one-way device, the network has no idea as to where the pager is, what it's doing, etc. so it just transmits each page all over the coverage area, every time.

"So?" you may say, "What's that do for me?" Well, it means two different things. First, pagers can be cloned with no fear of detection because the network just sends out the pages, and any pager with that capcode on that frequency will beep and receive the data. Second, it means that one can monitor pagers that are not based in their area. Based on the example of Dave's pager, he might have bought it in New York City. He also could live there. However, because the data is transmitted all over the coverage area, monitoring systems in Boston, Washington DC, and Philadelphia could all intercept his pages in real time. Many paging customers are unaware of their paging coverage areas and usually do not denote the NPA (area code) from which the page is being received. This can cause problems for the monitoring individual, who must always remember that seven digit pages shown on the decoder display are not necessarily for their own NPA.

The Pager Decoding Setup

Maybe you knew this, maybe you didn't.... Paging networks aren't encrypted. They all transmit data in the clear, generally in one of two formats. The older format is POCSAG; which stands for Post Office Code Standards Advisory Group. POCSAG is easily identified by two separate tones and then a burst of data. POCSAG is fairly easy to decode. FLEX, on the other hand, is a bit more difficult, but not impossible. FLEX signals have only a single tone preceding the data burst. Here's how to take those annoying signals out of your scanner and onto your monitor. You will need:

1. A scanner or other receiver with a discriminator output. A discriminator output is a direct connection to the output of the discriminator chip on your scanner. This is accomplished by soldering a single wire to the output pin of the NFM discriminator chip to the inner conductor of a jack installed on the scanner. RCA jacks are commonly used for convenience. A list of scanners and their discriminator chips can be found at http://www.comtronics.net/scandata.txt. For obvious reasons, the larger and more spacious a scanner is internally, the easier the modification is to perform.

2. A computer is required to actually interpret and display the pages. Most pager decoding software runs under Win95. This includes all software which uses the sound card to decode signals. If you have a data slicer, there are a few programs which will run under DOS.

3. You will need a Soundblaster compatible sound card. This will let you snag POCSAG traffic. Or you can build a data slicer and decode FLEX traffic too. Or you can be lazy and buy one from Texas 2-Way for about $80 or so. The Soundblaster method will obviously tie up your computer while decoding pages. Using the slicer will let you run decoders on an old DOS box and will let you use your better computer for more important stuff.

4. Antennas, cabling, etc.... You will need an RCA cable (preferably shielded) to take the discriminator output either into the sound card or into the slicer. If using a slicer, you will also need the cable to connect your slicer to your computer. As far as antennas go, pager signals are *very* strong, so you won't need much of an antenna. A rubber ducky with a right angle adapter, attached right to the back of the radio, will be more than enough. The signals are so damned strong that you might even be able to get away with a paper clip shoved into the antenna jack. Think of what kind of an antenna your pager has; this should give you a good idea of what the requirements are in the antenna department.

Connect your scanner's discriminator output to either your data slicer or your sound card. If using a sound card, be sure to use the line in connection. If using a data slicer, connect that to the correct port on your computer. Tune yourself a nice, strong (they're all strong, really) paging signal.

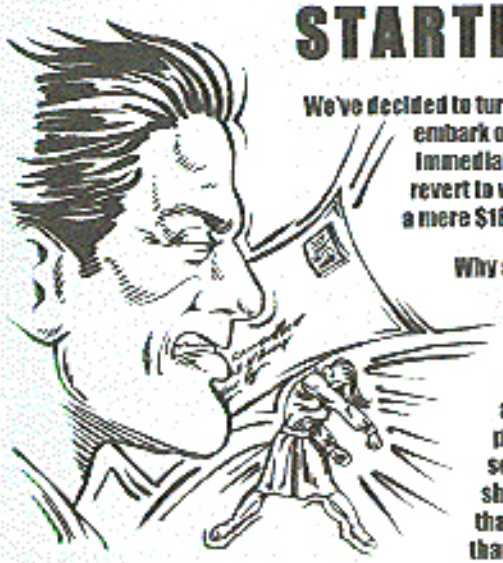
Where are they? Well, the vast majority of numeric pagers are crystalled between 929 and 932mHz. Try there. Or if you want to try decoding some alphanumeric pagers, try the VHF range around 158mHz. There is also some activity in the 460-470mHz range.

Now what about software, you say? That is where things start to get somewhat difficult. Motorola developed most paging protocols in use and holds licenses to them. Any software that decodes POCSAG or FLEX is a violation of Motorola's intellectual property rights. So one day, the people at Motorola decided that they didn't want that software floating around. They proceeded to look up everyone who had copies posted on the Web and told them that if they didn't take those specific programs off of the Web, it was court time. The threatened webmasters removed the offending copies, fearing a lawsuit from Motorola. After this, our good friends from the United States Secret Service arrested Bill Check and Keith Knipschild for messing around with decoding hardware and software - the SS appeared to want to make data slicers illegal. Of course, these arrests were ridiculous, but nobody wanted to get busted.... so the vast majority of resources on American websites disappeared. Checking around English or German sites may yield some interesting results.

Now you're ready. Fire up the software. Get that receiver on a nice, hot frequency. Look at all of the pages streaming across the network. Give it a few hours... getting bored yet? Yes? Okay... now that you have a functional decoding setup, let's make use of it. Know someone's pager that you want to monitor? Here's how to snag them... First you need the frequency; it's usually inscribed on the back of the pager. Also, you can try to determine what paging company they use, and then social engineer the freq out of the company. www.percon-corp.com also has a search function where you can locate all of the paging transmitters (and freqs) in your area, listed by who owns em. Not bad. So you have the frequency... now what? Well, wait until you have to actually talk to this person. Get your setup cranking on the frequency that this person's pager is using. Now, page him. Pay close attention to the data coming across the network... see your phone number there? See the capcode that your phone number is addressed to? That's it. Some better decoding programs have provisions to log every single page to a certain capcode to a logfile... this is a good thing. Get a data slicer, set everything up on a dedicated 486, and have fun gathering data.

For updates to this article visit the Phone Punx Network (http://fly.to/ppn). Mail can be sent to the Phone Punx address and it will find its way to me.

STARTLING NEWS



We've decided to turn back the hands of time and embark on a shrewd marketing ploy. Effective immediately, our subscription price will revert to what it was nearly ten years ago - a mere $18!

Why are we doing this? Have we completely lost our minds? We will not dignify that with a response. But we will say that we are looking to get more subscribers and, since the vast majority of people buy 2600 in the stores, this seems as good a way as any. Plus it'll shut up those people who complain that subscribing is more expensive than buying it at the stands. That's no longer the case. Now, in addition to not having to fight in the aisles for the latest issue and being able to place free marketplace ads, you will also save money over the newsstand price. Just like Time and Newsweek.

We're also lowering the price of our back issues. With every issue we stockpile, we lose more space so we'd really like to get rid of the dama things. You can now get back issues for $20 per year or $5 per issue from 1988 on. Overseas those numbers are $25 and $6.25 respectively.

Name: _____ **Amt. Enclosed:** _____

Address: _____ **Apt. #:** _____

City: _____ **State:** _____ **Zip:** _____

Individual Subscriptions (North America)

O 1 Year - $18 O 2 Years - $33 O 3 Years - $46

Overseas Subscriptions

O 1 Year, Individual - $26

Lifetime Subscription (anywhere)

O $260

Back Issues

$20 per year ($25 Overseas), 1984-1998

Indicate year(s): _____

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

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

HACK THE MEDIA

by Jim Nieken

Much has been said lately about journalists and the media, from their outright disregard for the likes of Kevin Mitnick and others, to MTV's much criticized foray into the lives of hackers. Few would deny the power and influence of journalists, yet no one seems to like them. They tend to paint hackers and most other "underground" subcultures in a negative light, and there are a number of reasons for this. Among them, deadlines and other time constraints, the betraying nature of the news gathering process, and the necessity to simplify information. But there are ways to turn the idiosyncrasies of journalism to your advantage, and to help reporters present an accurate and positive account. Follow my advice, and you might even find something good written about you in the paper.

First, some background. I have been working for various newspapers for years, both in freelance and staff reporter positions. My byline has graced the pages of papers both big and small, but I grew up working with local papers and tend to prefer them. I haven't done very much work with television, but the news gathering process is mostly interchangeable. Although a writer by trade, I am a geek at heart and must sympathize with the poor treatment my colleagues often give hackers.

This article is intended to explain how print and television journalists investigate and report a story, and what you can do if you are ever asked for an interview.

The Deadline: Your Ticket to Increased Adrenaline Output

Years ago, when I was just getting into the newspaper business, a grizzled old editor took me aside and explained what I was really supposed to be doing there. "My job," he said, "is filling up newspapers. Your job is meeting deadlines." His point was that while journalistic integrity was all well and good, newspapers couldn't print blank pages.

Deadlines are not just a part of the job; they are often the single most important concern. Reporters need to get their work in on time, and that can sometimes mean sacrificing accuracy for haste.

No one wants to print an untruthful story, but the fact is that the less time you spend researching, the less quality information you will get. That information also needs to be analyzed if it is to be conveyed correctly, which also takes time.

Looming deadlines are not the only factor in inaccurate reporting, but if you ever find yourself the subject of a story you should take them into account. If a reporter says that he or she has a day or less to cover a story, be concerned. If they have more than a few days they probably won't totally misrepresent you, and if they have several weeks the deadline is not likely to affect the quality of the reporting at all. This is why local television news reports are often so shoddy. Local TV reporters (carpetbaggers all) often work under deadlines of a few hours or less. They are told to run out to a location, pose in front of a building or a car accident, and rattle off a few facts provided by local law enforcement. They don't have time to actually investigate, which is the curse of all time constraints.

As a subject, there is little you can do about deadlines, but you may want to ask when their story is due. If you want to help yourself and create a better story, try your best to work within the limits of the reporter. If you just did something especially nasty to the local power grid and you would like your side of the story told before they haul you off to a holding cell, try to be available to media sources. You can't get your side out if you won't talk, and newspapers may be forced to print only what they have heard from other sources. Those may be your friends and family, but they could also be the police and other government agencies, or the guy whose life was ruined because he missed the season premiere of *Ally McBeal* when you took out the electric company.

The Interview as Seduction and Betrayal

In college, a journalism professor once told me that there are only two kinds of people in the world, those who are interviewed often and who know how to be interviewed - and those who aren't and don't. As a reporter I get most of my information via the interviewing process, but no other news gathering technique has a greater potential for distorting information. Unlike a school district budget, or the winner of an election, or something equally quantifiable, conversations are more subject to interpretation than most people realize. Your ideas must survive the transfer into your own words, into my head or into my notes, into new words in the final story, past the mercurial rempers of various editors, and finally back into the heads of a hundred thousand readers. It's not at all uncommon for people to complain that they were misquoted or misrepresented when they see their words in print. I hear it all the time.

The distortion extends beyond merely getting the exact wording of a quote wrong. Words are usually taken totally out of context, poorly extrapolated from sloppy notes, or even shamelessly fabricated. It's very uncommon for a reporter to totally fake quotes (we tend to be pretty anal when it comes to what's inside quote marks), but danger lies in how quotes are set up. It all depends on how your comments are explained and what context they are placed in.

You could say something like: "I don't really like people who break into other people's computers just to mess with stuff. I mean, the idiots usually deserve what they get for leaving stuff wide open, but it's really mean and no one should take advantage of people like that."

But a week later this might be printed in the local paper: "...One hacker said that he feels no sympathy for people whose computers are attacked or vandalized. 'The idiots usually deserve what they get for leaving their stuff wide open,' he said casually."

The quote was reproduced accurately, but the context was totally reversed. Beware of this. Reporters love juicy, callous, or controversial quotes. They spice up a piece of writing like you wouldn't believe. If you're not careful they could even end up right in the headline. If it takes three minutes of set up and hypothetical situations and philosophical justifications before you can say something like, "...so I guess if looked at it that way we should probably just blow up the phone company building," you can be assured they will not print the philosophical justifications and skip right into your admission of a terrorist plot.

As an interviewee, you can help in a number of ways. First, don't say anything that needs a lot of background or buildup. We work with sound bites, and you should never say anything you don't want printed unless you make it clear that it's off the record. All reporters will respect your wishes to not have a quote printed, but always pay attention to what you are saying. Don't say anything too sociopathic. Go slowly. We can only write so fast, and it allows you to choose your words more precisely. If you're ever suspicious, ask the reporter to read your words back to you. Make sure you like what it says, because they may come back to haunt you and this is the only chance you are going to get to change them. Also, always realize that you never have to answer any question asked by a reporter. We're not cops, and we can't force you to do anything. On the other hand, most journalists have large expense accounts and bribes are an extremely common industry practice. You might suggest that you sit down over dinner to talk. Be sure to order a dessert.

Journalists May Be Stupid, But Our Readers Are Even Stupider

My handy Microsoft Word grammar checker tells me that this document is written at or around the 10th grade reading level. This means that if you can read this paper without moving your lips, you are capable of reading at at least that level. Most magazines and nearly all newspapers are written at or around the 6th grade level. This is not because this is all the average American can handle. Rather, it keeps Joe Public from choking on his coffee at 7:30 AM as he slams into words like "axiological." Put simply - newspapers are mass mediums. They are consumed by the general public, and are written so people don't have to know anything about the subject being reported.

Newspapers are expected to provide only general information and basic facts. You might succeed in explaining the intricacies of exploiting a CGI loophole and stealing root access on a server to a reporter, but the writer still needs to explain that to 500,000 non-technical people. Most journalists are fairly good at assimilating information, but they are still not likely to get technical details correct. Even if they do understand it for some reason, it is likely to get twisted in the translation.

There is little you can do in this regard, other than to try simplifying your language. Assume that the reporter has no clue when it comes to technology, and no intention of printing anything the least bit technical anyway.

Journalism is a Business: A Lesson in Economic Theory

News reporting organizations are not a public service. They are a business like any other, and they must remain profitable if they want to continue printing or broadcasting. In order to do this, they must run interesting stories about interesting events. If that means slanting an issue or exaggerating a point, it can easily be justified. Most of my journalism classes in college centered on giving otherwise mundane stories enough "sizzle" to make them interesting. But there is a duality at work: "sizzle" versus "responsibility." Most reporters have no desire to print a false story, but most reporters have no desire to print a boring story either. Often the two sides are at least partially in conflict. But it could be worse than that, depending on the particular ethics of the organization doing the news gathering.

The journalistic reputation of the network or newspaper doing the story is typically a good barometer of how concerned they are about responsible reporting. I would trust PBS or *The New York Times* with just about anything, although they make errors like anyone else. I would trust the *Boston Globe* or the *Washington Post* to get most of the story right. I would expect the Associated Press, CNN, ABC, and the average local paper to at least get the basic information correct. I would bet some amount of money that CBS, NBC, MSNBC, Fox News, and most larger city papers retain at least a passing resemblance of reality. As for most Internet news clearinghouses, any local television news station, or the likes of MTV - their efforts are more akin to self-serving propaganda than journalism. I wouldn't trust MTV to report anything accurately, let alone something as delicate as what it means to be a hacker.

Every news-gathering company has a different perspective on sensationalism versus responsibility. It's probably in your best interest to evaluate how much you trust the particular organization before you consent to a story about or involving you. If you don't already trust most or all of what they tell you, don't expect that you and your story will fare any better. One thing you can do to help is to constantly mention how much you distrust the media and how they've let you down considerably in the past. Bring it to the forefront of the reporter's mind that accuracy is more important to you than what is provocative. Make him or her think that they will be betraying you if they misrepresent you in any way. It usually helps a lot.

Conclusion: Reporters are People, Too

If you ever find yourself the subject of a news story, be aware that the end product will probably not show you the same way you see yourself. Complicated details tend to be simplified, and that can mean a significant change for something as technical as computer hacking.

Like I said, no reporter and no newspaper wants to print an untruthful story. It's not likely that they will totally fabricate facts, but they can be taken out of context and reworked to create a more interesting story. Reporters often go into a story with preconceived ideas, and it can be difficult to change them. Just act natural, be truthful, and explain things as clearly as you can. If the reporter is any good, you may actually like what you read in the paper or see on TV a few days later.

PEOPLE WHO CAN'T KEEP QUIET

Inequities

Dear *2600*:

I was recently listening to the 5/17/99 *Off the Hook* and reading the latest copy of *Popular Science*. While looking through the ads in the back of *PopSci* I came upon the part in the show where you discussed the fact that DirecTV sued Dan Morgan for having information on how their technology works as well as ads for technology that bypasses their encryption and I noticed something. *PopSci*, a reputable and widely distributed magazine, runs ads for cable descramblers. These, as I recall, are illegal in most areas and have virtually the same function as the encryption bypassing technology advertised in *Satellite Watch News*. Upon further investigation I found that *Popular Mechanics* (*PopSci*'s sister magazine) also runs these ads. What the hell is the deal with this? Not to mention that the whole case violated the First Amendment and is complete and utter bullshit.

Ackbar

As this was a "civil" case, it was relatively easy for a large corporation like General Motors (you do know that General Motors owns DirecTV, don't you?) to shut down a puny publisher like "Satellite Watch News." In this case, the fact that SWN dared to print articles detailing how DSS signals could be decoded was enough to incur GM's wrath. Even with the First Amendment and many loyal subscribers on one's side, it can often be impossible to survive the litigation that a corporate giant can muster. By the way, we will cheerfully print any articles on the subject of decoding DSS signals.

The Politics of Hacking

Dear *2600*:

About the letter in 16:2 by RGBKnight, I've come to the conclusion that most of the people in "hacker groups" are just idiots wanting people to worship them so they can step on them. All it is is posing by a bunch of jerks who want everybody to know how "elite" they are. Real hacking takes place behind closed doors with people who don't want publicity or social recognition, who learn for the sake of learning. Personally I don't participate in any of the bunko jobs that seem to pass for "hacking" nowadays like warez trading or even electronic breaking and entering. I determined long ago that America's "educational" system is really an indoctrination system and that if you want to learn anything useful you have to learn it yourself. My goal in what I call hacking is to learn as much as I can about technology, including but not limited to that which is forbidden for the sheep to know. In a society in which knowledge is forbidden, knowledge is truly power. I don't belong to any groups, I don't seek approval from "peers" or posers. I learn for the sake of learning. About Kevin Mitnick, I think that the real crime he committed is not that which he was charged with (or even what he was not charged with). What he pled to was rather small potatoes. Social engineering doesn't deserve four and a half years in prison. But I know what the government thinks does deserve it: Mitnick's forbidden knowledge. Simply put, Mitnick knows too much for the rulers' comfort. As I said before, when knowledge is forbidden it is power. I dusted off my copy of *The Fugitive Game* a few days ago, and right on the back cover Mitnick says: "They're saying that I'm John Dillinger, that I'm terrific, that it's shocking that I could get this awesome power... People who use computers are very trusting, very easy to manipulate. I know the computer systems of the world are not as safe as they think."

That is Kevin's real crime: exposing the fault lines in the power of the ruling class. Therefore, we should say that he is proudly guilty as charged, and that the government's Orwellian psychological torture experiment on Mitnick is just a symptom of how fragile their hold is on those who have the knowledge. Free Kevin for the sake of Kevin, but also to show that the Power can be fought successfully. Kevin Mitnick and Bernie S. have already shown us that it is truly We the People, and not They the Rulers, who have the power - when we have the knowledge. And that, not social recognition or publicity, is the true purpose of hacking.

Desaparecido

Well said.

Dear *2600*:

Thanks for letting us see what can be done. I am an East Timorese myself and was glad to see that we can protest in so many ways to get our message across. Just wanted to say thanks for letting me see how I can protest. Never thought about it. Cheers.

long live xanana
FT 4 1 ife
phillip

While the leaked Indonesian web pages (which according to our archives date back to 1997) may not have been the final straw in sparking a successful uprising, they did open up some eyes that the authorities preferred to keep closed. That is itself shows the potential value of such a means of expression.

Dear *2600*:

This is in reply to the letter in 16:2 about how this anonymous person refused to steal from a cable truck saying that he/she didn't want to damage their karma (or get caught). Not only did this person not take anything, but he/she left the door open to the truck so the driver would come back and see that someone had been in it. This way the driver would learn a lesson and not keep the door unlocked again. Now there are some people who believe that that is the right and moral thing to do. I'm not necessarily patronizing these people but here is my side.

This anonymous person said, "My hacking philosophy has usually been one of education." This is my philosophy as well. If I steal equipment out of a cable or Bell truck, I could educate myself by examining it, or maybe even use it for some phreaking phun. If I were to steal any handbooks out of these trucks, then I definitely would be educating myself. There may be valuable information in these books that I could not find anywhere else. By doing this I don't believe that "A life of crime is my goal." Yet a life full of knowledge and excitement is.

I think this is important to talk about because stealing for the sake of knowledge is a subject that hackers and phreaks on any level can disagree upon.

TeckX3
BRONX

You raise an interesting point. We strongly believe that obtaining knowledge of how something works isn't a bad thing. But if you then use that knowledge in a destructive way, that is where you've gone wrong. As for how the knowledge is obtained, that too can make a big difference. If you shoot and kill a technician because you want to read one of his manuals, the knowledge isn't so much the issue as is how you obtained it. Same thing with breaking into a van to steal something. You're actually physically breaking into something and you're depriving someone of something that is theirs (stealing). That's far different from copying it or tricking the company into sending you a copy. In desperate times, stealing can be the only way to survive. We just don't believe it's quite at that point yet.

Dear *2600*:

This is in response to nobody's letter in 16:2. I must say I am in complete agreement. Sadly, in this day and age most everyone judges a book by its cover. Therefore, to further advance our causes, I think it is vitally important to remain ever so "underground" even if that means (shiver) conformity on the outside. After being involved with computers for quite a few years now and also involved with the general public, I have found it is far easier to get what you want and get away with it if people feel you are like them. If wearing Tommy Hilfiger and Calvin Klein keeps people from being suspicious and even judgmental, then by all means have at it. Nevertheless, keep doing whatever you want in your own time. Then again, if you feel it is necessary to spike your hair three feet over your head, dye it purple, and pierce every loose piece of skin you possibly can (I am being very stereotypical here and sport eight piercings myself) then by all means please do. However, I and many more like me, feel it is far more beneficial to beat society at its own vain and superficial game.

Major Motoko

This works fine if you're going "undercover" for a specific project. But many people expand this to include their school, work, and family life, all for the sake of making things easier. Only problem there is that the more you play that game the more you need to. When your designer jeans turn into mortgages you find it much harder to turn on the idealism when you feel like it. If you don't sell out your values from the start, you'll find it a lot easier to hold onto them in different situations. You might also be surprised how much you can get away with while being "weird."

Difference of Opinion

Dear *2600*:

I read the informative article in the CNN Internet section (cnn.com/TECH/specials/hackers/qandas). I believe it was your editor who responded to the questions by CNN. I really do appreciate your honesty and candid response. I am a person who believes that the government and the corporations have been misleading us for decades. There is much evidence that this is true. I do not believe that everything I read or see on a web site is accurate. On the contrary, being a thinking person, I take everything that I hear or read with a grain of salt. Being a thinking person, I feel I should respond to your response. First off, I believe your logic is quite flawed. Pagers, cell phones, and computers are primarily communication devices. They are not toys. According to your mentality it is okay to steal something if others leave it out in the open. Your philosophy leaves much room for the justification of breaking and entering, and copying web pages that don't belong to you. One could perceive your actions and the actions of all of your group as the selfish behavior of individuals who have very little respect for the privacy of other individuals. In response to your opinion that hackers should not be prosecuted and put in prison it's not surprising considering that most criminals do not understand why they are in jail. We as a society cannot let our private belongings and documents be subject to the criminal class. As long as your organization believes it has the right to steal from others (just because you can) and take advantage of new technology to the detriment of your fellow brothers and sisters, I will never support hackers or their belief systems. It is interesting that you feel you are doing this country a great service by being the first to break in and rearrange legitimate web sites, believing that if your organization did not do it first, that international terrorists would get around to it. But that is not the way it happened, is it? Unfortunately, your organization has become the terrorists you say you so adamantly oppose.

Jeffrey Stollman
Milwaukee

PEOPLE WHO CAN'T KEEP QUIET

Inequities

Dear *2600*:

I was recently listening to the 6/17/99 *Off the Hook* and reading the latest copy of *Popular Science*. While looking through the ads in the back of *PopSci* I came upon the part in the show where you discussed the fact that DirecTV sued Dan Morgan for having information on how their technology works as well as ads for technology that bypasses their encryption and I noticed something. *PopSci*, a reputable and widely distributed magazine, runs ads for cable descramblers. These, as I recall, are illegal in most areas and have virtually the same function as the encryption bypassing technology advertised in *Satellite Watch News*. Upon further investigation I found that *Popular Mechanics* (*PopSci*'s sister magazine) also runs these ads. What the hell is the deal with this? Not to mention that the whole case violated the First Amendment and is complete and utter bullshit.

Aekhar

At first was a "civil" case, it was relatively easy for a large corporation like General Motors (you do know that General Motors owns DirecTV, don't you?) to shut down a puny publisher like "Satellite Watch News." In this case, the fact that SWN dared to print articles detailing how DSS signals could be decoded was enough to incur GMC's wrath. Even with the First Amendment and many loyal subscribers on one's side, it can often be impossible to survive the litigation that a corporate giant can muster. By the way, we will cheerfully print any articles on the subject of decoding DSS signals.

The Politics of Hacking

Dear *2600*:

About the letter in 16:2 by RGBKnight, I've come to the conclusion that most of the people in "hacker groups" are just idiots wanting people to worship them so they can step on them. All it is is posing by a bunch of jerks who want everybody to know how "elite" they are. Real hacking takes place behind closed doors with people who don't want publicity or social recognition, who learn for the sake of learning. Personally I don't participate in any of the bunkin jobs that seem to pass for "hacking" nowadays like wance trading or even electronic breaking and entering. I determined long ago that America's "educational" system is really an indoctrination system and that if you want to learn anything useful you have to learn it yourself. My goal in what I call hacking is to learn as much as I can about technology, including but not limited to that which is forbidden for the sheep to know. In a society in which knowledge is forbidden, knowledge is truly power. I don't belong to any groups, I don't seek approval from "peers" or posers. I learn for the sake of learning. About Kevin Mitnick, I think that the real crime he committed is not that which he was charged with (or even what he was not charged with). What he pled to was rather small potatoes. Social engineering doesn't deserve four and a half years in prison. But I know what the government thinks does deserve it: Mitnick's forbidden knowledge. Simply put, Mitnick knows too much for the rulers' comfort. As I said before, when knowledge is forbidden it is power. I dusted off my copy of *The Fugitive Game* a few days ago, and right on the back cover Mitnick says: "They're saying that I'm John Dillinger, that I'm terrible, that it's shocking that I could get this awesome power... People who use computers are very trusting, very easy to manipulate. I know the computer systems of the world are not as safe as they think."

That is Kevin's *real* crime: exposing the fault lines in the power of the ruling class. Therefore, we should say that he is proudly guilty as charged, and that the government's Orwellian psychological torture experiment on Mitnick is just a symptom of how fragile their hold is on those who have the knowledge. Free Kevin for the sake of Kevin, but also to show that the Power can be fought successfully. Kevin Mitnick and Bernie S. have already shown us that it is truly We the People, and not They the Rulers, who have the power - when we have the knowledge. And *that*, not social recognition or publicity, is the true purpose of hacking.

Desaparecido

Well said.

Dear *2600*:

Thanks for letting us see what can be done. I am an East Timorese myself and was glad to see that we can protest in so many ways to get our message across. Just wanted to say thanks for letting me see how I can protest. Never thought about it. Cheers.

long live xanana
ET 4 Life
phillip

While the hacked Indonesian web pages (which according to our archives date back to 1997) may not have been the final straw in sparking a successful uprising, they did open up some eyes that the authorities preferred to keep closed. That in itself shows the potential value of such a means of expression.

Dear *2600*:

This is in reply to the letter in 16:2 about how this anonymous person refused to steal from a cable truck saying that he/she didn't want to damage their karma (or get caught). Not only did this person not take anything, but he/she left the door open to the truck so the driver would come back and see that someone had been in it. This way the driver would learn a lesson and not keep the door unlocked again. Now there are some people who believe that that is the right and moral thing to do. I'm not necessarily patronizing these people but here is my side.

This anonymous person said, "My hacking philosophy has usually been one of education." This is my philosophy as well. If I steal equipment out of a cable or Bell truck, I could educate myself by examining it, or maybe even use it for some phreaking plan. If I were to steal any handbooks out of these trucks, then I definitely would be educating myself. There may be valuable information in these books that I could not find anywhere else. By doing this I don't believe that "A life of crime is my goal." Yet a life full of knowledge and excitement is.

I think this is important to talk about because stealing for the sake of knowledge is a subject that hackers and phreaks on any level can disagree upon.

TeckX3
BRONX

You raise an interesting point. We strongly believe that obtaining knowledge of how something works isn't a bad thing. But if you then use that knowledge in a destructive way, that is where you've gone wrong. As for how the knowledge is obtained, that too can make a big difference. If you shoot and kill a technician because you want to read one of his manuals, the knowledge isn't so much the issue as is how you obtained it. Same thing with breaking into a van to steal something. You're actually physically breaking into something and you're depriving someone of something that is theirs (sending). That's far different from copying it or tricking the computer into sending you a copy. In desperate times, stealing can be the only way to survive. We just don't believe it's quite at that point yet.

Dear *2600*:

This is in response to oolong's letter in 16:2. I must say I am in complete agreement. Sadly, in this day and age most everyone judges a book by its cover. Therefore, to further advance our causes, I think it is vitally important to remain ever so "underground" even if that means (sliver) conformity on the outside. After being involved with computers for quite a few years now and also involved with the general public, I have found it is far easier to get what you want and get away with it if people feel you are like them. If wearing Tommy Hilfiger and Calvin Klein keeps people from being suspicious and even judgmental, then by all means have at it. Nevertheless, keep doing whatever you want in your own time. Then again, if you feel it is necessary to spike your hair three feet over your head, dye it purple, and pierce every loose piece of skin you possibly can (I am being very stereotypical here and sport eight piercings myself) then by all means please do. However, I and many more like me, feel it is far more beneficial to beat society at its own vain and superficial game.

Major Motoko

This works fine if you're going "undercover" for a specific project. But many people expand this to include their school, work, and family life, all for the sake of making things easier. Only problem there is that the more you play that game the more you need to. When your designer jeans turn into mortgages you find it much harder to turn on the ideatine when you feel like it. If you don't sell out your values from the start, you'll find it a lot easier to hold onto them in different situations. You might also be surprised how much you can get away with while being "weird."

Difference of Opinion

Dear *2600*:

I read the informative article in the CNN Internet section (cnn.com/TECH/specials/hackers/qanda). I believe it was your editor who responded to the questions by CNN. I really do appreciate your honesty and candid response. I am a person who believes that the government and the corporations have been misleading us for decades. There is much evidence that this is true. I do not believe that everything I read or see on a web site is accurate. On the contrary, being a thinking person, I take everything that I hear or read with a grain of salt. Being a thinking person, I feel I should respond to your response. First off, I believe your logic is quite flawed. Pagers, cell phones, and computers are primarily communication devices. They are not toys. According to your mentality it is okay to steal something if others leave it out in the open. Your philosophy leaves much room for the justification of breaking and entering, and copying web pages that don't belong to you. One could perceive your actions and the actions of all of your group as the selfish behavior of individuals who have very little regard for the privacy of other individuals. In response to your opinion that hackers should not be prosecuted and put in prison it's not surprising considering that most criminals do not understand why they are in jail. We as a society cannot let our private belongings and documents be subject to the criminal class. As long as your organization believes it has the right to steal from others (just because you can) and take advantage of new technology to the detriment of your fellow brothers and sisters, I will never support hackers or their belief systems. It is interesting that you feel you are doing this country a great service by being the first to break in and rearrange legitimate web sites, believing that if your organization did not do it first, that international terrorists would get around to it. But that is not the way it happened, is it? Unfortunately, your organization has become the terrorists you say you so adamantly oppose.

Jeffrey Seelman
Milwaukee

There's nothing like a letter that starts off really nice and then plummets into name-calling and foolish simplicity. Now let's try and stay civil. We do not condone theft. However, your definition of theft is so incredibly broad as to include things like copying web pages! You need to realize what theft really is - taking something away that isn't yours to take. Simple enough? When you take something, it's not there anymore. Copying a file isn't the same as taking it. Now you can argue that this doesn't make it right and maybe that's true. But it doesn't make it equivalent to whatever crime you want to punish people for. As for your little rant on our inability to respect privacy, perhaps you should look at who is invading yours. How much junk mail do you get from hackers? How many times have we entered your name into a database and shared it with several thousand of our friends? How many times have we left your private info lying around for anyone to stumble across? Hackers have learned these things through exploring and refusing to believe everything they're told. Hackers encourage the use of encryption in order to further protect one's privacy. Take a good look at who opposes strong encryption and direct your anger that way. We're sorry you don't think of pagers, cell phones, and computers as toys but we always will and it's from that enthusiasm that we will design applications that you would never dream of. That is entirely your loss. You may think it's appropriate to imprison people who don't buy into your values and occasionally embarrass powerful entities. We don't.

Dear 2600:

First thing's First i know since im on aol i'm a "lamer" or Whatever you wanna call me but im also on mIRC...but the Reason im writing this letter is because i wanna FuCK up AOL and i found some Stupid String to make "guides" "host's" "rangers" and "ims" if 2600 put's this in a Mag the Strings might be dead Cause they change them monthly but since im SuCH a HaCKeR if you need them or need the new one's if there Dead Email me @aol.com use Subject "aolsucks" or something Gay like that well here are the String and go OSW the FUCK outta some Guides =] Gudie String=NMF. Host=ISV Ranger=OLA im=WPI.

KeeP it ReaL in tha 9e9 and PHrEAK the Fuck outta some PHoNeZ for me

Da "Sleep"

You watched the MTV special, didn't you? Anyway, you really need to hook up with the writer of the letter before yours. There's no end to what the two of you could teach each other.

Mitnick

Dear 2600:

Congratulations to Kevin Mitnick, the 2600 team, and everybody who played a part in spreading the word. Justice still evaded Kevin, he was by no means treated fairly, and the remaining aspects of his sentencing are still unacceptable given his time in jail without bail/trial. But the matter, save his probation, will soon be behind him, so we can at least celebrate that. I look forward to listening to Kevin alongside Bernie S. on *Off The Hook* sometime in the future, and I look forward to replacing the "Free Kevin" bumper sticker on my car with a "Kevin is Free" sticker. A good job all around.

EchoMirage

We hope you're making the stickers this time round.

Dear 2600:

Over the summer I was a counselor at a national computer camp (Oglethorpe University in Atlanta) where I taught 16/32 bit Intel x86 assembly, c, c++, and Pascal to around 250 kids. During the two weeks that I taught and had fun (it was a blast surprisingly), I would sit down daily with a group of my students during breaks and explain to them the whole Mitnick affair, what happened, what went wrong, etc. I've never seen so many little kids filled with such enthusiasm on a political/ethical issue such as this. It was awesome the reactions that were raised from our discussions. Now there are some 250+ kids ranging from 8-13 or so running around in Atlanta with an insanely enthusiastic Free Kevin mentality about them, which can only help the situation. I think that we (as in those who back Mitnick and want to fight the hell he's going through) should try and educate the upcoming generation on the whole affair whenever the opportunity arises. I think a lot of times people just try and target an older generation because they can do something about it right now, rather than the generation who in five or six years will have the power to make a difference. We have to think of the future, not just the present.

skaboy

Good point. And in case anyone in Atlanta was wondering what all the noise was, now you know.

Dear 2600:

The lesson taught by the U.S. government prosecution of Kevin Mitnick should clearly show that all hackers should unite for the common purpose of bringing down the U.S. government through the disruption of its computer systems. There is already a replacement government ready. It's manifesto can be observed at: www.angelfire.com/on/clonemperor/index.html. Thank you.

Don L.

Well now that the replacement government is ready, what are we waiting for?

Dear 2600:

I just wanted to let you know that while I was at school one day, we had a guest speaker from the FBI. He was a Special Agent from the Kansas City Branch. When I asked him about his thoughts on Kevin, he didn't say much. This got all my other classmates wondering who Kevin was, and he still wouldn't talk about it. It's like the agents are told not to talk about him. He did say that he thought that Kevin deserved the time that he got, and that was about it.

CherryPie

It took a lot of guts to speak up like that. The things some kids are doing in school today are a real inspiration to us.

Dear 2600:

I found your article "Slow Motion" very interesting. I had not previously seen any articles that detailed the recent history of Kevin Mitnick. I found the money issues to be quit enlightening and almost laughable. I wonder how many others suffer similar fates, yet remain anonymous.

BADJRM

Too many, we're sure. We will try to keep updated on as many as possible.

Dear 2600:

How in the world do you actually think the Mitnick case is unfair when there are so many more unfair cases in this world? Kevin, sorry to say buddy, but you are the least of anyone's concerns. There are people right now on death row. And you are sitting here in a little jail cell getting money from big time nerds who think you are their shrine. How can you tell me that you think five years is bad compared to someone who is right now on death row for life and every week you are getting a letter saying this is the last week of your life. Well Kevin, sorry buddy, we do not care that much about five years of your bad life. That five years would be like heaven compared to one week on death row. So why are you guys promoting it so it won't happen again? Stop trying to raise money for this one guy. We are not playing favorites over here. Let's get some money to all of the people in jail, not just one dork who got busted for computer fraud or whatever he got charged with. I subscribed to 2600 for years and years. Then finally the whole book is a Kevin Mitnick book I'm paying for. Do us a favor. Just drop it.

matt

The only thing more annoying than people who don't care are people who pretend they do. We doubt you really give a shit about anyone who's suffering so just drop the facade.

Dear 2600:

I was recently reading a letter written by Brother Inferior in issue 16:3 about how the Mitnick case and the Mumia Abu Jamal case are so closely related. Let's think about the facts for a moment. Mumia is in prison because he murdered a cop (whether out of cold blood or self defense.) Mitnick trespassed on computer systems and caused $4000 of damage (who did it affect, that Chinese dude, and now he's a millionaire). How can we even think that these two cases are at all related? Mitnick did something that really hurt no one and Mumia did something that affects the family of the cop, the police force, and probably a lot of other people. You do Mitnick a disservice trying to relate the two people. So stick to your skate mags, and don't buy 2600 any more.

Darth_tampon

In case our response to that letter somehow was smudged, we'll repeat the gist of it here. It's not so much the actual guilt or innocence but the fact that when you see the authorities distort the truth and abuse the system as we have seen with the Mitnick case and others, it becomes much easier to take other such claims seriously whereas those who never question the authorities would never consider this for a second. It seems quite apparent that there are more than a few improprieties in the prosecution of the Mumia case - the wide assortment of people around the world calling for a new trial is something that should be taken seriously. And, for the record, Shimomura is Japanese.

Dear 2600:

I happened to be in the parking lot of the Navy Hospital in Beaufort, SC today and saw a car with a "Free Kevin" bumper sticker on it. I've been following the story since I first read it in 2600 and explained it all to my wife. We are both glad that it is winding down but are still angered over the treatment of him. I was just amazed that your outreach is so far, that bumper stickers turn up in the craziest places.

Also in the 16:2 2600, ethan wrote about a secret in Excel 97. There is also one for Excel 95 for those of you who haven't upgraded yet. Go to line 95 and select it. Hit the tab key once. Then click Help, then About. Now hold down SHIFT ALT CTL and click on Tech Support. There you are. Now you can explore all around and check it out. If you go to the wall to the left of where you start and move up against it, then type EXCELKFA, the wall will disappear, and you can continue up the path. If you make it outside, let us know what's out there. I keep falling off the damn ledge.

Suicidal

Stupidity

Dear 2600:

I was glancing through some of amazon.com's more interesting books when I noticed a link at the bottom of the review inviting the author to submit his comments. Curious, I followed it, wondering what kind of verification system they'd have to keep ne'er-do-wells from impersonating some poor writer. As it turns out, they ask you once, politely, if you are indeed the author, after which you're pretty much free to post whatever you want. I've currently "authored" several books and I still cannot believe security could be this lax. I stuck mainly with obscure technical and conspiracy books, but I don't see anything stopping your readers from penning such masterpieces as *The Bind* or *The Collected Works of Shakespeare*. Note: All I had to do was find a book without an author review and go to it. As long as you stay within the rather loose submission guidelines, Amazon will post the most bizarre author comments. But try not to rag on a writer too much. These guys have to make a living too. Expect your comments to be posted in 5-7 days.

kipple

You're absolutely right about the shoddy verification on Amazon. We were a bit skeptical at first so we decided to try it on one of our favorite titles. Within days, "How To Become a Pokemon Master" had our rather cryptic remarks attached to its Amazon entry, no doubt confusing and inspiring kids all around the world. We're curious what other odd remarks will pop up between now and the day Amazon wakes up.

Dear *2600*:

I was watching C-SPAN on Sept. 20th at about 8 pm, and Matt Drudge and Mike Kinsley (of slate.com) were being interviewed by the show's usual guest, Brian Lamb. After his usual political conspiracy rantings, Drudge launched into an attack on hackers, calling them wimps. He tried to get Mike Kinsley to join in, but he'd have none of it. Drudge claims that it's "hackers" who messed up his vile web site dedicated to scandal, yellow "journalism," libel, innuendo, and sensationalism. He also gloated that he railed against hackers on a radio show (I'm not sure if he was a guest or if he now has his own show). He also all but called them cowards.

I'm not shocked that an amoral nitwit like Drudge would liken "hacker" to a person who acts in an illegal fashion. Nor am I shocked that he'd lump them all together. What does shock me is that he was stupid enough to challenge "hackers" to hack his site again.

Jack O'Lantern

Think how bad we'd all feel if he said he liked us.

Dear *2600*:

Recently, I was perusing my October 5, 1999 edition of the *Orlando Sentinel*, the local paper for most of us in the Central Florida area. On page A 11, in the Op-Ed section, Leonard Pitts of the Tribune Media Services had an article about how Vietcom chief Sumner Redstone said the news media was being insensitive to Chinese and Cuban leaders. Mr. Pitts was very sarcastic with all of this and then made a general apology to "all the nation's swindlers, drunken drivers, hackers, car-jackers, robbers, rapists, stalkers, murderers, and molesters." He then goes on to say "Hey, just because they're the scum of the earth doesn't mean they don't have feelings." Now guess which group of people he mentioned that pissed me off the most. At the end of the article, the *Sentinel* says that "readers can contact Leonard Pitts via e-mail at elpjay@aol.com or by calling him toll-free at 1-800-457-3881." I encourage everyone with the time to contact him and explain in a mature and intelligent manner that hackers do not belong in the same category as rapists and murderers. If you can't explain your position to him without being a moron, don't e-mail or call him.

Dr. Bagpipes

Dear *2600*:

In the November 8, 1999 *Business Week*, page 6, I noticed an anecdote entitled "The List: Justice American Style." Part of the blurb reads: "Half of all Americans say that they would act on their own beliefs of right and wrong..." Basically, nullification (which by itself might not be a bad thing), "regardless of legal instructions involved with controversial issues, products or services."

Mildly interesting, to be sure. The plot thickens. Of the six prejudices jurors would not be able to overcome - as you might expect, white supremacists, gun manufacturers, tobacco companies, breast implant manufacturers, and HMOs were on this list — "a computer hacker" placed second, a mere 12 percent behind the white supremacist and five percent above gun manufacturers, some with tobacco, and eight percent above both breast implanters and HMOs.

You're so right about the insanity of this country towards inquiry. Kevin might be a hard luck story readers can contrast with on an abstract level, but these kinds of surveys should wake the hacker community up to the fact that the public is now gunning for you.

e. edward kelso
***FISTICUFFS* zine**

Dear *2600*:

I work for a financial services company here in the UK. Recently I was part of an evaluation effort on a product called Session Wall. This is a straight scanning program that can filter by content type and either block, log, or warn an admin of sites. The categories are as you would expect: Sex, Terrorism, and so on. One category which caught my eye was "Criminal or Subversive Content". The IT guy said that the settings for the blocked sites were as the product came out of the box. The only two sites listed as Subversive or Criminal were www.2600.com and www.kevinmitnick.com.

Thought you'd like to know.

Arcoddath
Scotland

OK, we're convinced. Nobody likes us.

Dear *2600*:

There's a simple bug in the proxy software we have running here at work and I'd guess that it's available in most proxy software. We're running a program called Cyber Patrol that can restrict access to web sites that are deemed inappropriate but it only matches a list of www.*.* strings and not IP addresses.

Any idiot can figure out that resolving the IP address and manually entering it in your web browser will still get you to the page (simply ping aol.com, get the IP address and you're on your way). A bug this large shouldn't be allowed in something that claims "Cyber Patrol is the Internet filtering software rated the best by educators, industry and leading magazines" (www.cyberpatrol.com).

Anubis

Handy Stuff To Know

Dear *2600*:

If you go to www.mapquest.com and get a map by searching by area code and prefix, the star should be the location of the CO for the exchange. Seems to work in most of the cases. It's very cool!

J. Arthur Ballarat
Los Angeles, CA

We found this to be amazingly accurate in just about every exchange we entered. What a great way to find the location of your central office!

Dear *2600*:

Ya, ever heard of www.freei.net? There's a thing I discovered in it where you can surf without the damn ads. Here's how: After you download the software and sign-up and shit, just open up the program as usual, then wait until it loads completely. When you see "Freei Networks" on the taskbar, right click it and select "Close". When it says "Disconnecting from Freei. It may take a few minutes" or something like that, press Ctrl+Alt+Del and select 'Goodbye from Freei' and press 'End Task'. When the "End Task" prompt shows up, press "End Task", and voila! The Internet connection stays and the ads go away.

I'm only eleven years old, by the way...

mad kow diseez

And already figuring out how to defeat commercialization of the net.

The High Cost of Learning

Dear *2600*:

I found out how screwed up this world is over the course of two to three weeks. I minimized this window that comes up on boot up. The librarian went over to the computer and freaked out and rebooted it. Later in the day when I went back to the library, she pulled me aside and asked me why I messed up the computers. I was like what the hell. She threatened to give me two days of in-school suspension if I didn't tell her what I did to mess the computers up. Also, my friend asked about Kevin Mitnick and if they had any books about him. The librarian freaked again and made him walk through the little scanner thing two times and empty his pockets to make sure he didn't steal anything. The world has all the wrong ideas about us. I think it is stupid to think that we all have malicious intentions. What do you think about this?

gpf

Stupidity breeds in schools.

Dear *2600*:

I would like to add another incident to the ever growing "guilt by association" section. I was also caught in school reading your zine when I got sent to the office for a lecture and apparently marked as a computer ruffian. First I was accused of stealing a Macintosh camera, which they later discovered was the doing of someone else. Then I was accused of "hacking" on a teacher's computer, when it didn't even have a modem. After that I was told that I had "made an alias hard drive" on one of their Macs which was complete crap. I don't even know what the hell that is, if it's even an actual term or even possible. I have no experience with Macs whatsoever. Yet I got banned from my computer lab and sentenced to a month of ISS (in school suspension). I slowly fell behind because of the school's apparent apathy about my further education (you see, they don't let you out of ISS until you are completely caught up with your work and you've completed your term). I flunked the grade because of that. After a rough start in the next year of high school I dropped out. I think that the whole Mitnick case has put quite a paranoid spell over many people. Seems as though the media dropped the topic when the tables were turned. The government has made quite an example and 1984 is just around the corner.

hightechno

Dear *2600*:

Why are people so afraid of hackers? People in my school are afraid. I'll do something to their credit or something, and I never even threatened any of them. I'm starting to wish I did.

Valen

Understandable but you must resist the dark side.

Mysteries

Dear *2600*:

In the lot beside my apartment complex there is a BellSouth building. I've never seen anyone go through the front door or come out of it, but I have seen a few people driving out of the barbed-wire gates in the evening. The building has no windows, flood lights on all sides, and the front door (which is glass) opens into a very small, empty room with another door. The second door is significantly heavier (wood or metal) with one of those swipe-card security boxes. There is no office or secretary, and I'm not sure why they even have a front door. What is this place? I imagined it was some sort of substation thing but why does it look like a maximum security prison? What is so important inside that they have razor barbs around? Are they just really paranoid about vandalism?

drdoom

This sounds like a central office where calls for the area are switched. It could also be a toll station used for routing long distance. Since that is the heart of the phone system, the security is understandable. Many central offices these days require little in the way of human presence which would explain why people are seldom around. You can use the method another reader submitted above for tracking down your central office to see if that's what it is. If it isn't, keep asking questions until someone tells you. You have every right to know.

Dear *2600*:

In the main library of my city, I saw that they changed the old Windows NT computers to computers from Sun Microsystems running Solaris. The interface sucks ass and the keys are misplaced. I found out that if you press alt-b and type anything you want, you'll get a gray screen that says: "Whatchew talkin' 'bout, Willis?"

I wonder what is that?

Jack

From what we're told, this has something to do with the financial difficulties "Different Strokes" star Gary Coleman has gotten into. Since he gets a royalty every time that line is used, his financial standing will soon be restored. Your library will receive a bill every time you do that with the help of the secret locator chip that comes with all upgrades.

Hotmail Hijinx

Dear *2600*:

In 16:2 Letters, ZeROLogiKz wrote about hidden text located at the top of Hotmail's website. His assumption was that Microsoft was "withholding" information from viewers. That's not the case at all. What Microsoft was doing was attempting to improve their search engine listings, by stooping to the level of a spammer.

Hiding text in web pages is fairly common practice, and it's done by matching the text color to the background color. The hidden text will usually have something to do with the topic of the page itself and oftentimes, it'll be nothing more than large groups of similar words. The idea is to pad the page's content with extra instances of key words, in hopes of being listed higher in search results. Case in point, at Hotmail, the hidden text talked about "Free Email (Electronic Mail) on the Internet."

You'll find the same phenomenon at most porn sites - visit any porn site and do a Select All. Chances are you'll find a huge string of hidden words, e.g. "ass tits sex fuck" etc. The site's webmaster has placed these words on the page, hoping that his site will be listed first when someone heads to Altavista and searches for something nasty.

Of course, what most webmasters obviously don't realize is that these search-engine spamming tactics don't work. Search engines, for the most part, aren't run by idiots; and the folks who operate the major search engines are always installing new filters to combat spam. For example, most search engines now check for the presence of a BGCOLOR tag in every page, and will *ignore* any text that's set to the background color. Some engines take this a step farther and ignore text that's anywhere near the background; e.g. #F3F3F3 text on a #FFFFFF background would be ignored. Most search engines also filter out words which recur too often, large groups of words with no punctuation, etc.

You'd think that Microsoft of all companies would know that hidden text is the most outdated (and useless) trick in the book. Regardless, I guess what surprises me most is that Microsoft would even *want* to spam the search engines like some shady porn site. As if there's a person on the planet who doesn't already know what Hotmail is - or where to find it.

Shaun
Memphis, TN

Retail Tips

Dear *2600*:

I am sure you have all seen the credit card boxes in most stores. They have an LED message bar at the top, a numeric keypad, and a place to swipe the card. I have seen them almost everywhere, including Blockbuster, Wal-Mart, and Ingles. They are out on the checkout counter for all the patrons to use. The heart of these machines is a simple modem setup. Hmmm, modem. The modem calls the store's system, wherever it may be, each time a credit card is used.

Here's the kicker. The setup program for each modem is accessed through the credit card boxes! I found this out by accident one day while messing with the box in Blockbuster. After trying different key combinations, I was prompted with the setup options on the little green LED screen! I reset the modem, and the system hung. The idiots working there were like "What the fuck happened?" As it turned out, they apologized for a "power surge" (heh) and gave us our rentals for free!

So I know what you are thinking, "That's great, but how do I do it?" Well, the answer is simple. Every one of these machines is made by the same company, and therefore there is a default key sequence that will enter setup on most any machine. By default, no password is requested, however I have encountered machines with password protection (in Wal Mart). To enter setup you must press the upper right and lower left keys simultaneously, then the lower right and upper left keys simultaneously. This should get you into setup on 90 percent of all boxes. If you find that the box is password protected, often it is the store number which is on all receipts. I have rarely encountered protected ones. Apparently, most stores think that all the protection they need is an obvious key sequence. Typical.

Once you are in, there are plenty of options, such as changing the number to dial, resetting the modem, setting the baud rate, and even better stuff. I am not telling you this, though, so that you can steal credit card numbers, this is to simply give you more knowledge. If you steal credit card numbers, you are reflecting poorly on yourself *and* the hacker community, so don't. Have fun with this, and keep information free.

Willy L. AKA Yerba

This is an excellent example of what the hacker community stands for. In the eyes of the ignorant, there is no other use for this information except to commit a crime. There is nobody at our office who upon reading this didn't immediately head over to the 24 hour supermarket to try this out. It's what you do with the knowledge that determines what kind of person you are. There are those who would already condemn you for telling us and certainly they would condemn us for telling the world. Playing around with such a system may get you into trouble but it's little more than curiosity and experimentation, both healthy things. Now, if you rig the thing to call a number and approve your fake credit card, you become a thief as soon as you start stealing. That defines where we draw the line, at the actual commission of a crime. Not the spreading of information, not the theorizing, not even the experimentation. Vandalism and theft are easily defined yet our critics want to muddy the waters by extending their definitions to encompass speech and simple mischief. All this will accomplish is to create a whole new population of so-called criminals. Unfortunately this seems to be a growing trend.

Dear *2600*:

Recently I was in Borders Books and I really wanted to get this Linux book with a three disc set but it cost 70 bucks. I only had 30 on me. It just so happened that there was an older edition of that book that was only 29.99. I swapped the price tags. When I went to the front counter, the lady didn't even think twice when she asked for 30 bucks. I started to get really curious about this. I came back the next day and found another expensive book but this time switched the price tag with a book on a completely different subject. I went to the checkout and the lady said it was the wrong tag and she had to look up the real price. A few days later I was at CompUSA and they had two versions of visual c++; professional, which was $450, and learning, which was $80. I switched those tags and it worked.

SenorPuto

Good one. Now try this. You can avoid the hassle of paying entirely by simply running out the door while holding the item you wish to take. This may result in loud noises, shouting people, and sirens of various sorts. We suggest experimenting as much as possible and keeping a log of what different stores do. And if by some bizarre twist of fate you wind up in a courtroom, show the judge this letter. They need to laugh too.

Dear *2600*:

Caspla add-ons to finn's letter about ATMs and OS/2 in 16:3. OS/2 is very widely used in banks. NationsBank and Bank of Boston being two of the biggest. In addition to banks, POS systems use OS/2, as he/she stated in his letter about Kinkos. Take a look next time you are at Ruby Tuesday or a bar with a touch screen system, eight out of ten times it'll be an OS/2 driven system.

creature

Update:

Dear *2600*:

This is in response to "the ninth name is NOD's" letter about the worst in www.whatisbomatris.com. There are other names that you can type in too. I just viewed the source and it came up with these: geef, skroce, darrow, wring number, guns, morpheus, trinity, deja vu, steak, agentbullettime, crash, lobby, mirror mirror, neo bullet time, SENTINEL, NEBUCHADNEZZAR, SENTINELLARGE800x600, and site credits.

kAoS

Dear *2600*:

In response to a letter from chart in 16:2, the newer version (3.0) of AIM will not let you hex the advert.ocm file and get away with it. I tried hexing it as usual. Then I saved it. When I brought up AIM and signed on, I noticed nothing had changed. I got back into the Hex editor and found that the original file was restored. I don't know if AOL reads *2600*, but somehow they figured it out and found a way to ditch it. If anyone knows how to get around this, please let us know. Anyway, since reading that article, I've been hexing all my programs that have ads in them including Juno and GoZilla.

Sirblime

Dear *2600*:

Another Bell Atlantic update. Their recently upgraded voice mail has a special feature. Try dialing 7 or 9. This used to be used for moving back or forward through a message. Now when you press 7 or 9 you can hear parts of other people's messages. Messages that are from someone else's voice mail entirely! Another innovation brought to you from Bell Atlantic.

Loggia

We strongly suspect this was a temporary problem and that it was only in your area's system and not in every system, at least not at the same time. However, it's yet another reason why getting voice mail through the phone company is a pretty dumb move.

Dear *2600*:

To check your long distance carrier (inter-LATA), you use, as always 1-700-555-4141. The new number to check your *intra*-LATA carrier is 700-4141 (just the seven digits).

dannyb

You can actually enter any four digits after the 700 for this new number. In addition, you can sometimes get some rather interesting results - in some areas we've heard an ID from NYNEX, a company that hasn't existed since 1997.

Dear *2600*:

A letter from Corl.an published in 16:2 told of a little string which will make a pop-up ad pop right back down again afterwards. Well, there's an easy way to keep the darn thing from popping up at all. The HTML {noscript} tag does what it says - it turns off scripts until the tag is undone ({/noscript}). Well, since the pop-up ads are popped up by java scripts, a well placed {noscript} tag will keep the script from ever happening. For those who use Tripod, the script is automatically placed in the {head}, so putting a {noscript} before the head (and a {/noscript} after, if you use scripts later on in the page) will do the trick. Incidentally, no ad will pop up if you simply do not use a {head} tag at all, but that's usually not practical. If you also use scripts in your {head}, it shouldn't be too hard to figure out where exactly the script goes, and place your {noscript} and your scripts strategically. (I think you can put a {noscript} after the

(hide), and then put your scripts, but I'm not sure.) For those of you unfortunate enough to be using Geocities, I believe the script is put at the very end of the page, so just slip in a (noscript) at the end. Personally, I prefer to use the many free web space providers that are actually *free*, with no ad requirements or anything.

Sir Reginald

Dear *2600*:

I am writing in response to the article in your last issue about hacking the gated community TV/phone entry box. Whoever wrote this ought to be shot for giving such little info. I looked all over my apartment building's box for the manufacturer, but it wasn't displayed. Luckily, the box broke soon after that and a repair technician was dispatched. When he arrived, I went right up and asked him who manufactured the box. He also let me have a peek inside. He said it was the Series Systems, Infinity "I." Series. You can download information about these machines at www.seriessystems.com. I found that it is rather simple to dial into these boxes if you set up your terminal properly. You must use TVI 910 emulation. No, all you Win 95 losers, you can't use HyperTerminal. Get a real term prog. Set data bits and parity to 8/N/1, XON/XOFF, and the manual also says full-duplex (FDX) but I didn't need to set that in mine. The baud rate is tricky so you may need to reconnect at different speeds starting from 14400 and working your way down until you get it right. The particular box I was dialing into gave up the handshake without any further configuration, but the troubleshooter's manual I downloaded from the website states that some units are configured to require a "*" followed by a six digit access code before the handshake starts. Fortunately, the factory default is 000000. The backdoor code for pre-1994 models is 736859. There is no logging mechanism for dial-in, so a late-night brute force broken over several nights should work also. This same code can be used from the keypad to enter "program mode". Just type "***" and then the six digit code. Once inside, there's not much to do. You can make the door open at certain times if you want or change the clock time. Although it is pretty cool that instead of my last name, my friends have to scroll down to SATAN when they come over.

Wishing he was back in New York

Dear *2600*:

Regarding the article on Infiltrating MediaOne, if I may correct a few points... The biggest error is the password thing: MediaOne's default password is never "password" and if the tech that set this up set it to that, he's a moron and probably doesn't work there anymore. In my experience it's always been HSD then a random number, and I think they've changed it since then. Also, you can call tech support and change your password that way, not just through the web page. There also seems to be this strange idea that MediaOne doesn't like people running Linux. They actually don't care what you run, but the techs are only trained to do installations on Windows and Macintosh systems. Once they leave you can plug it into your Linux box, call up tech support, tell them your new mac address, and you're good to go. But if you have a problem you're out of luck, because they don't support Linux, and also the box has to be locked up from hacker activity. They do random scans for open ports and potentially illegal activity. And lastly, the print and file sharing thing is not valid. All modems have the ports for that blocked out and the only way to get them removed is to ask for them to be removed.

Sc00ter

Dear *2600*:

In "Internet Radio," theJestre recommends portscanning the Real Audio server to get the port it's running on. It would be a hell of a lot easier to just connect to the server, netstat -a, then pick out the connection you're looking for. The single connection would look a heckuva lot less suspicious than an entire portscan on a 2000 port range. (By the way, I've found many servers on port 7070.)

emdeo

Dear *2600*:

I just wanted to add a little bit of info to AE0u99's modchip/Game Enhancer letter. First, there are a few different versions of modchip, and if you're duped into buying an older one, you'll find most newer games don't work. The latest version uses the Stealth program, which is only detected by the newest Japanese games and a very few cruddy American releases. So the stealth modchip is perfectly viable right now. I own one. The Japanese version of FF8 detects the stealth modchip, but Square (good guys, them) removed it for the American release. My guess is they realized they'd be locking out a good portion of their audience.

If some game you want to play detects a modchip, you can either use a game enhancer code that fools the modchip detection used in the game, or apply a simple patch to the ISO image you're copying. These can be found all over the web, and are mainly for PAL/NTSC conversions. A note about using game enhancers exclusively instead of modchips, though: I've read that you cannot use them to play multi disc games. A second note: modchip burners can be made for less than $20 and the software is freely available. I recommend going this route if you're in for a challenge. If not, I bought my modchip from www.gbxtance.com and am completely satisfied.

On the complete opposite end of the spectrum now, I'm enlisted in the Air Force, and they do use TEMPEST in buildings and computer systems that deal with classified information. However, we aren't told anything about it other than the fact that it exists. I don't work around anything classified (heh, or so I'm led to believe), so snooping around probably wouldn't do any good. But I certainly will write if something interesting ever pops up.

Ed

Dear *2600*:

I must have had a slip of the fingers in my letter to you. The phone test number in Long Beach, CA is 117 (not 1170 like I wrote). Did it, wait a moment, and a voice will come on the line saying something like "Tracker Test..." and then give you a verbal menu of all the tests you can do by pressing the numbers (it's a long list).

SAR

Dear *2600*:

Hey, remember that trick for Hotmail where you could get into someone's account if they were logged in? Hotmail fixed it immediately but there is another way. However, it is hard to implement. You need netbus or some other remote admin tool where you can get a screen dump. When you are logged into Hotmail, you will notice in the location box a bunch of gibberish. If you can get a screen dump while your victim is logged in to their account, and you type the gibberish into your location box, you can get into their account as long as they are logged in!

hidden101

Otherwise known as jumping through hoops.

Dear *2600*:

In response to your 15:1 article "Hacking a Sony Playstation" and the letter from matt in 16:2, I would like to follow up. First, if you look on the bottom of your PSX, in the top right corner of the label, you will find the model series. The Playstation has evolved throughout the years - from changing the position of the laser, changing the writing on the button etc. - but in essence it is still the same (although the 1000 series is supposed to be slightly faster). I myself am the proud owner of a 1002 model. However, onto the point. The late 7000's and the 9000's have, as matt said, a steel case over where the mod chip would go, but all the models (even my 1002) have a parallel port, where I stick my "GameBooster." This lets me play imports, copies, and GameBoy carts. Very useful. I got mine for 315 pounds (yes, England). Another method to playing imports and backups is the disc swap. Press Open, and find the button at the back that detects the cover is shut, then stick in a pencil, blu-tak it to the top, and voila. Now stick in a regular game, wait for the piracy screen, then rip it out and stick in a copy/import. This is risky though; you have to rip out the game while it is spinning, and I will take no responsibility if you screw up. On a side note, if you own a 1000 and the laser has packed in, or you notice decreased performance, turn the Playstation upside down. May sound crazy, but it works.

CuS

Suggestions

Dear *2600*:

As I was reading your magazine the other day I remembered the U.S. Navy Seals and everything they do for us. Please have a section honoring the U.S. Navy Seals. Thank you.

Black Knight

We'll devote a whole issue to them if you tell us how in hell we reminded you of them.

Dear *2600*:

I don't know if you are in a position to answer this but I thought I would give it a try. I am completely fed up with rude people and their cell phones. Especially people who can't resist answering and talking on them in movie theaters, restaurants, etc. An inability to drive and talk at the same time is also high on my list. I was hoping to find plans for a box that would automatically disconnect cell phones or cause so much static that the owners could not use them. Given my limited understanding of how cell phones work I expect the easiest option would be to create a great deal of static by transmitting noise across the correct frequency range. Making them call back and adding up connect charges several times before they give up would be very satisfying. Even better would be the ability to make it ring again and again until they turn it off but I'm fairly sure that is not possible.

Russ

Dear *2600*:

I just picked up your Fall '99 issue a couple of days ago. Great stuff. I always get excited when I peruse through your mag and find code, especially socket code. I'm a beginner socket programmer, and any articles that have code in them really help me out (the socket programming articles in 15:3 and 16:1 got me started). If I could just ask one thing of people who submit source code for their articles, it's to please, *please*, add comments to your code. You may be able to understand it, but others may not. Thanks again, and keep up the good work!

sureshot

Ripoff

Dear *2600*:

On this month's telephone statement (Bell Atlantic) I noticed there was a $5 charge for switching long-distance carriers. The switch was from MCI WorldCom, address in Denver, to WorldCom Inc., with an address in San Antonio. As we know, these companies are now the same company.

I called to complain, received a credit and apologies, of course. But I wonder how many MCI WorldCom customers will be billed for a nonexistent switch to WorldCom and pay, not noticing the problem.

Larry

Observations

Dear *2600*:

I'm not sure if you've gotten letters like this before, but I thought this might be of interest. I've noticed a little

continued on 48

HOW TO CREATE NEW URBAN LEGENDS

by Jim Johnstone

Urban legends are fantastic stories people tell each other. They hear the story from a friend, who heard it from someone else, and so on. The result is the same as playing that kid's game of telephone: the stories evolve, often becoming funnier, scarier, or sicker. They also take on local characteristics, sometimes naming local streets or cities or even names of people. And, of course, they become impossible to verify.

The growth of the Internet has provided an ideal medium for the transfer of urban legends. They can now be e-mailed to people around the world quickly and easily.

Common Characteristics of Urban Legends

Many urban legends contain similar characteristics. Usually they have a moral to tell. "Don't do this" or "Watch out for this." Many e-mailed legends coerce people into sending them onwards, often by using guilt or appealing to a sense of ethics. Some legends are downright gruesome. They tap into our subconscious fears causing us to exclaim, "I knew it!" Other urban legends contain subtle and overt humor. (Like the story of the woman who found a stray dog in New York City. She took it in to her home, fed it, washed it, bought it a flea collar, and took it to the vet. The vet examined it and told the woman she had actually caught an oversized wharf rat.)

Three New Urban Stories

The Excited Chiropractor

This happened to my friend's chiropractor instructor at a college in Vancouver, BC. He said that one day during class the president of the college walked in and announced that the professor had been promoted to head of the department. Everybody clapped and congratulated the beaming man. Later that night when he went home and announced his good fortune to his family he was so excited that he gave his five year old son a big bear hug. He heard a terrible cracking and the boy was rushed to Vancouver Public General Hospital. The x-rays revealed that the boy had fractured three lower lumbar. (A broken back.) Not only did the chiropractor instructor not accept his new promotion, the next day he tearfully announced to the class that he was resigning immediately.

Analysis: Any story where a kid dies or is hurt gets passed around by anxious parents. This story works because it's ironic. It's a chiropractor of all people who broke his kid's back. He goes from being on top of the world to resigning in disgrace, all in one day. The story also plays on people's fears about cracking backs. Every story needs a hook that makes people pass it around.

Moral: Don't hug people too hard, especially if you are a chiropractor who just got a promotion.

The Miracle Diet

My aunt's friend worked with a woman who was always trying these crash diets. One day she came across a small classified ad for a revolutionary pill that guaranteed rapid weight loss. She paid and was sent the pills in the mail about a week later. To her delight she started losing weight. Slowly at first then faster and faster. She went from 200 pounds to 125. Unfortunately, by the third month, she was feeling more and more nauseous. One day her doctor took some x-rays of her intestines and found a three-foot tapeworm growing inside her! The diet company had sent her a pill infested with tapeworm eggs. She was given anthelmintics, a drug that kills worms, and put on a diet high in iron salts. The salt caused her to gain all her weight back, and she ballooned again to 215 pounds.

Analysis: Have you ever imagined what it would be like to have a three-foot worm attached to your insides, slurping up all the food you just digested? You probably have. I just took this fear and escalated it. To add some humor, I made the woman gain all the weight back as punishment for her being so goddamn stupid.

Moral: Don't try miracle pills or crash diets. Also notice how I used the word anthelmintics. Using jargon makes your story more believable. (I also used jargon in the chiropractor story with lumbar.)

Man Dies Proving Internet is Safe for Children

AP - Jesse Solomon, 55, died yesterday after a bomb that he was building exploded in his arms near Flagstaff, Arizona. Solomon was apparently proving to a friend that the Internet did not provide dangerous information about how to construct bombs, Molotov cocktails, and poisonous substances.

Jason Riggs, Solomon's friend, said the two had been arguing the week before about the dangers of the Internet. "I told him that children could find stuff that could do a lot of damage. I said the net should be more regulated." According to Riggs, Solomon disagreed. "I downloaded a text file about how to use household chemicals to make a bomb right in your kitchen," said Riggs. When he showed Solomon the information, Solomon denied that the recipe would work. "He called it a hoax and an urban legend and said that he would prove it to me."

The next day Riggs was phoned by Flagstaff police and asked to identify the body of his friend. Constable Samantha Heathers said that an ambulance was called to Solomon's residence after neighbors complained of an explosion. Police found remnants of a makeshift bomb and evacuated two nearby apartment buildings. Solomon was taken to Hotel Dieu Hospital but was pronounced dead on arrival.

"He was trying to prove to his friend that the instructions for making the bomb were bogus," said Heathers. "People should be very cautious about what they receive on the Internet," she added. The police are still investigating the incident.

Analysis: You will notice right away that I made this story sound like a news report. Don't be afraid to try different styles. In this case, a news report adds credibility to an otherwise unbelievable story. Again, I used humor and irony as the catch. The big thing going for this tale is that it panders to society's fears of technology.

Moral: The Internet is evil.

Creating your Own Legend

Watch out. Some people will be upset at you for creating yet another untrue legend that circulates through society. There is a mass movement on the Internet of people dedicated to debunking urban legends (see Barb Mikkelson's website - www.snopes.com and the Computer Virus Myth's page - kumite.com/myths). They think we waste our time passing on useless stories or hoaxes - it's also annoying logging on to your e-mail account to 50 messages, half of them silly stories that have been forwarded to hundreds of people before you. Then again, almost everybody enjoys a good tale.

Generally folklorists don't think it's possible for people to make up an urban legend. Jan Harold Brunvand, author of several popular books on urban legends, believes that true legends develop from people changing details of a story until the story develops its own oral tradition. Scholars call this process communal re-creation. But if your story is clever enough, it might get e-mailed to hundreds of different people and develop its own tradition.

Okay, so how do we do it? Just think of a good story. Make it funny,disgusting, not too unbelievable, and perhaps add a moral. Say that it happened to your friend's mother's dentist. Keep it local, use street names if possible. I strongly suggest that you *don't* make it cute and cuddly. There is nothing more annoying than reading about some women who met the man of her dreams and blah blah blah. Keep it vicious and sadistic - for entertainment purposes! Feel free to use the ones I just made up or change them to your liking. Once they're out there, you can forget about copyright or anything like that. They are in the public domain. Just remember that by creating urban stories (they're not legends yet!), you're not exactly making the world a better place to live.

U.S. DEPARTMENT OF JUSTICE
Federal Bureau of Prisons

E

STAMPS, NEGOTIABLE INSTRUMENT, OR OTHER ITEMS RETURNED TO SENDER

To (Name - Set Return Address)
PO Box 752
Middle Island, NY 11953

From (Institution)
FCI LOMPOC

Inmate's Name
Mitnick, Kevin

Register Number
89950-012

Date
10/8/99.

Material Returned

(Check One)

___ You enclosed with your correspondence stamps or stamped items that cannot be given to the inmate.

___ You enclosed with your correspondence an incorrectly prepared negotiable instrument. (Negotiable instruments require the inmate's committed name and register number.)

___ The below material cannot be ingested without damage

___ Electronic Musical Greeting Card

___ Padded Card

___ Dyed by Food Polaroid Photos

___ Other - specify below

✓ You enclosed unauthorized material:

___ Body Hair

___ Plant Shavings

___ Sexually Explicit Personal Photos

✓ Other - specify below

The correspondence or letter has, however, been provided to the inmate with a copy of this notice.

Specific Material Returned

2" of internet, web-site material printed in code.

(Printed/Typed Name and Written Signature of Legal Technician)

DISTRIBUTION:
Original - Address (with mail)
Yellow - Inmate
Pink - Mail Room File
Goldenrod - Central File

BP-S384.052
JANUARY 1991

While we managed to suppress the urge to send body hair and plant shavings, we just couldn't resist sending two inches "of internet, web-site material printed in code." That happened to be Kevin's e-mail that we've been sending him for years which has helped to keep him sane all this time. To these people, anything they don't understand could be considered a "code" which pretty much includes it all.

Hacking Explorer [the car]

by Bob

Since I only have my own vehicle I can't be sure if this will work on earlier/later Explorers or any of Ford's other vehicles with keyless entry systems.

Entry

Given that the Explorer in question has a keypad entry system let's begin. The numbers on the keypad will range from 1 to 0 grouped in pairs of two. For instance: {1-2} {3-4} {5-6} {7-8} {9-0}. These keypads come preset with a five digit permanent code, which you can change if you so please. Unfortunately the permanent code still stays in memory. I've learned that you can hit any amount of numbers beforehand as long as you get the code in the right order. So you can pretty much punch random numbers without stopping for any length of time and not set off alarms, and still be allowed entry if you get the code in the right order. Also, hitting the {3-4} button after the code has been entered and the driver's side door unlocked (it does this automatically when the code is punched in) will unlock all the doors. Turning the key twice within four seconds in any of the car's locks also has this effect.

Getting the Code

Ford is very stupid if the following is true. The nature of the last three digits of my entry code, "911," made me think that Ford may actually preset their numbers to have this as the last three digits so that it will be easy to remember. If this is so then "XX911," where "XX" is any two number combination, would be the format to use in hacking the code. This will greatly reduce the hacking time. If this is not the case then the fact that you can just keep pressing buttons randomly until it unlocks, instead of having to wait five seconds before trying again, makes Ford seem rather stupid as well.

Now What

Now that you have the code you get to decide what to do with it. You could change the code on the door, but that's useless because you can still use the permanent code. Nevertheless, here is how to go about adding your own personal code (useful for flaunting your power over a friend).

Enter the permanent code. Within five seconds press the {1-2} button. Within five seconds of that, enter the new code. To erase a personal code, repeat steps 1 and 2 but skip step 3 (wait six seconds).

The car's alarm system (if equipped) can be armed from the keypad by pressing {7-8} {9-0} and disarmed by simply entering the code. The Autolock feature (if you or your friend is cheap) can also be disabled and re-enabled using the keypad. Just enter the permanent code (not the user set code) and within five seconds hold the {7-8} button and then within five more seconds press and release the {3-4} button. (No, you can't let go of the {7-8} button - you just have to stand there and look stupid.)

Just for Fun

Even without the entry code you can still lock all the doors on the car by holding in the {7-8} and {9-0} buttons at the same time. You can also set your friend's seat (if equipped) to all the way forward (if they are tall) or all the way back (if they are short). First, turn the car on. Then move the seat to the desired position. Press the set button, the light will come on. While the light is on, press control 1.

And while you're plucking with your friend's car, make sure you slap a "Free Kevin" bumper sticker on the back too. Have fun!

Net Nanny Nonsense

by Raz

Net Nanny is one of those many Internet "surveillance" programs for Windows that is designed to allow parents to monitor and restrict their children's computer usage, and children are pretty much the only people who will be restricted with this. This program is so shoddily made I don't know where to start. So I'll just walk you through a tour.

Internet Monitoring

Net Nanny is supposed to watch web browsers, and any other programs parents define, for any content that is deemed offensive to kids. It has a list of web sites, newsgroups, and words or phrases that it looks for, plus the parent can add anything they want. First of all, as of Net Nanny 3.10, it doesn't even work with Netscape 4.5 or higher, so if you plan on using that, don't even think twice about this program. It does work, however, with Internet Explorer (I tested it with version 5).

Getting into Net Nanny

If the default installation settings were used, Net Nanny will be in C:\NetNanny and there will be shortcuts on the desktop and in the Start Menu if you run Net Nanny, then it will prompt you for the password. Type it in wrong and it goes into the log. In the folder where it was installed, you will find six programs (one to configure, one to administer, one to remove the program, and a few others), help files, readmes, dlls, and then some files needed by Net Nanny to run. After a little experimenting with time stamps, I found that Wnn3b.dat is the most important file. It contains all the lists of words or sites to look for, user names, their passwords, and the administrator password. Uh oh, I accidentally deleted it. Will Net Nanny now crash my computer, or lock me out of the system? Of course not. Net Nanny is user-friendly. Just run it and instead of asking for a password it will tell you there is none, and ask you if you would like to set a new one. Sure you would.

That will work for getting into Net Nanny to administer. If you just want to browse the web without being restricted or logged, just do the old Ctrl-Alt-Del and close the program named Wnldr32. Also, by simply moving or deleting Wnn3b.dat from the Net Nanny folder, it stops Net Nanny from blocking or logging any Internet connections, be it web sites or irc channels or whatever.

This all could be fine for some people - just delete the file or close the program and you're done. But others of you out there may want to be a little more discreet about your computer usage, or actually change the Net Nanny settings. First, I suggest copying Wnn3.log to another folder. This is the log file, and keeps track of everything relating to the Net Nanny program with time stamps. Now, there are a few ways to get into the Net Nanny program. The hardest way is to move the file Wnn3b.dat somewhere, then start Net Nanny. Then make a password and exit. Move the new Wnn3b.dat and do it all over again, but this time with a different password of the same length. Now you have two Wnn3b.dat files of the same size, each with a different password. Everything within the files is encrypted, so you can't just open it up and change the password. But, if you open up the two files in a comparison program, you can see where in the file the difference is, thus what part of the file the password is kept in. Once you know where it is, you can open up the original Wnn3b.dat in a hex editor, go to that part, and replace it with the same part of one of the other files. You now have a copy of Wnn3b.dat with the original settings, but a different password. Just move it back to the Net Nanny folder and you're on your way. It would probably be best to also keep a copy of the original file, so you can replace it if your parents or whoever administers it has to get into it.

An easier, and probably the best way, to get into Net Nanny would be to move Wnn3b.dat somewhere, start Net Nanny, and make a new password. Now you have two Wnn3b.dat files: one for your use, and one for the person who thinks they're in control. You could just switch them whenever you want to use it, and then change it back when you're done. I say this is the best way because now you can control it to your liking, but still easily change it back when needed.

By far the easiest way to take control of Net Nanny is to just reinstall it. If you don't have the disks your parents used to install it, you can just go to www.netnanny.com and download their 30 day evaluation. Reinstalling Net Nanny resets everything back to the original, so it's just like when your parents first installed it.

Surveillance Programs in General

I did not intend this article to be solely about Net Nanny. It is by far the worst of these types of programs I have seen yet. I really just wanted to give people an idea of how it worked, and perhaps other programs out there work the same way. Here are some things that will work with any of these programs, simply because they rely on human weaknesses instead of the program's faults.

A First Grade is to see how gullible your parents are is to open up the monitoring program in a hex editor and change words like "OFF" to "ON", "Enabled" to "Disabled", and vice versa. When they open up the program and see that it's offabled (really on) they might try to turn it on, not knowing that they are actually disabling it for you. Another good one is to fill up your autoexec.bat file to print on the screen that the monitoring program is in serious error, and failure to do so will most probably lead to hard drive failure (or something along those lines). Finally, the oldest tricks are sometimes the best. A key logger hidden in the background will tell you the password the next time someone tries to get into the program.

If you do find that whatever program your system is running has a main file where it keeps all its information, and if you get into the program and change the settings and/or password, you should copy it somewhere safe and set your system to copy it to the program's folder at startup. This will insure that your settings will always be there, unmolested. Good luck!

Why Redboxing Doesn't Work

by The Prophet

To understand why redboxing doesn't work, it is important to understand why it did at one point work (and still does in some areas), and to understand the various types of payphones and toll collecting systems.

There are two major types of payphones. Standard fortress payphones utilize a ground start and ACTS toll collection mechanism, and are usually operated by the incumbent local exchange carrier (ILEC) in any given area. Examples of ILECs are USWest, GTE, Pacific Bell, etc. Such phones are usually manufactured by Western Electric or GTE, although in Alaska and Canada you still find some old brown post-pay Northern Telecom payphones. COCOTS (Customer Owned Coin Operated Telephones) are operated primarily by private payphone owners. However, ILECs operate COCOT-ized payphones of this type. BellSouth's operations in southern Florida are an excellent example of this. The primary difference between a "standard" payphone and a COCOT-type payphone is that with a "standard" phone, toll collection and verification is based in the central office. With a COCOT-type phone, it is handled by the telephone itself. This is a very important distinction, which you will appreciate later. There is another type of fortress phone, which is post-pay. You see these only rarely used, in some parts of Canada, remote areas of the US, and in Alaska. I won't go into how post-pay phones work since they're so rarely seen.

Let's briefly consider how a standard fortress payphone works. To make a local call on a standard payphone, you insert the amount of money required. In this area, it's 35 cents. After you deposit 35 cents, the payphone grounds itself. This "ground start" indicates to the central office that the proper amount of money has been paid and the central office lets the call go through. If you didn't put in the correct amount of money, then you'll be routed to a recording instructing you to deposit 35 cents before making your call. Because the ground start mechanism is not dependent on any tones, you cannot redbox local calls - unless you route them through a long distance carrier. Sometimes this is possible; try dialing a carrier access code before your local call. As an interesting sidenote, residential phones don't have a ground start mechanism, which can create very amusing results if their line class is inadvertently changed to that of a payphone.

Long distance calls are a little more complicated. It costs less money to call Portland, OR (503) from Seattle than it does to call Gander, Newfoundland (709) from Seattle. About $3 less for the first three minutes, in fact. Additionally, toll rates are not flat, and they vary by time of day. Clearly, a ground start mechanism isn't a good way to bill such calls. You can only set one fixed amount for ground start calls, and you can't easily limit the time, either. Recognizing this, payphones are equipped with a tone generator which plays an appropriate pulse to indicate the type and quantity of coin you've dropped in.

It used to be that when you placed a long distance call, an operator would come on, inform you of the charge, and then would listen to and write down every coin that you dropped into the phone (there is one pulse for a nickel, two pulses for a dime, and five pulses for a quarter which is how the operator could tell what you were depositing). She would proceed to connect your call upon your deposit of the correct amount, and would either collect the balance at the end of the call, or would break in every few minutes to get you to deposit more money. But with the golden age of layoffs and computerization, ACTS was born. ACTS stands for Automated Coin Toll System. It does the job of an operator by listening to the tones generated by the payphone when you deposit coins and tallying them appropriately. However, it's a computer and is not as smart as an operator. This is where redboxes come into play.

A redbox is, quite simply, a device which generates the same coin deposit tones - and loosely the same

timing - as a payphone. Contrary to popular belief, it's not necessary to modify a Radio Shack tone dialer with a 6.5536MHz crystal to create a redbox (6.49MHz is a far better frequency anyway). You can record the tones directly from a payphone to a voice mailbox and record them to a Hallmark greeting card or a micro-casette recorder, and that will work.

Whichever method you use to create a redbox (I won't belabor the point of how to manufacture one, there are plenty of instructions elsewhere), its purpose is simply to fool ACTS into thinking you're putting money into the phone.

ACTS has rapidly disappeared over the past few years. The primary reason for this is the FCC. With the 1996 telecommunications bill, the FCC ruled that ILECs may not offer any services to their own payphone divisions which they do not also offer to independent operators of CO-COTs. This made offering ACTS and ground start billing problematic, since ACTS would have to be upgraded to charge different rates based on each COCOT operator's criteria. Additionally, it would have been necessary for ILECs to handle separations and settlements for the COCOT owners. This was a bigger job than ILECs wanted - especially to maintain a system which was increasingly plagued by toll fraud.

As a result, many ILECs began replacing their phones with Northern Telecom Millenniums, or COCOT-izing their Western Electric payphones (such as what BellSouth did). Because the billing is all done in the phone itself, rather than via ACTS, there is no need to fool ACTS any longer. Therefore, you can play tones at a COCOT or a COCOT-ized ILEC phone all day and it won't work. Also, some ILECs who kept ACTS (usually by offering it to COCOT owners but making the fees so high that nobody took advantage) such as Pacific Bell have installed filter chips in their fortress phones. These filters block the handset microphone until the call supervises, which does an effective job of blocking redboxing.

Redboxing does still work in some places. However, it's eventually going away. What really should go with redboxing are access charges - since long distance ought not be billed by the minute anyway. But I digress....

Spoofing Call Waiting ID

by Lucky225
Lucky225@hotmail.com

In this article I will explain how Caller ID on Call Waiting (Call Waiting ID) works and how it is possible to display messages on Caller ID equipment.

How It Works

When you have call waiting, you will notice that you hear two tones if you have Call Waiting ID. The first is the Subscriber Alert Signal (SAS or "call waiting beep") tone. This is just your normal call waiting beep (440hz for 330ms). The second tone is a CAS (CPE Alert Signal) tone. This is a short 80ms DTMF tone of 2130+2750hz. This tone alerts the CPE (Customer Premise Equipment, in other words, the Caller ID box) that there is a call waiting tone. The CPE then mutes the handset and sends an acknowledgment tone (DTMF "A" or "D" tone) to the central office to tell the CO that it is OK to send Caller ID information. Next, the central office sends out Caller ID information in FSK format. The name and number are displayed on the CPE and the CPE unmutes the handset.

Spoofing

To send a fake message to be displayed on the Caller ID box you will need a recording of an FSK transmission. We are currently working on a program that will create an audio file with whatever information you want. If you would like to help please e-mail me. In the meantime you can do the following. Order Call Waiting ID or go to a friend's house who has it. Call your phone when it's in use so you get a call waiting beep. *Make sure there are no CPE's on the line.* When you hear the CAS tone send an acknowledgment tone back and the central office will send the FSK signal over the line. Record this with a micro-recorder or some other recording device. Once you have your FSK recorded, call the person you want to put the CID message on and play a CAS tone. You'll hear his CPE chirp back with a acknowledgment tone. Then play your recording of the FSK signal. If you did it fast enough the information will show up on his caller ID screen.

Obtaining Tones

You can make an orange box (CAS tone generator) by modifying a tone dialer. Just take out the 3.58mhz crystal and put in an 8.192mhz crystal and the star button will create a CAS tone!. You can make acknowledgment tones by creating a silver box (plans easily found on the Internet).

The Sprint Integrated On-demand Network (ION)

by Prototype Zero
prototype0@collegeclub.com

Recently I happened upon a lot of information on Sprint's new ION technology. I decided to share this info with my community. ION stands for Integrated On-demand Network. The basic idea of ION is to provide customers with unlimited numbers of phone lines, etc. The system works by dynamically allocating bandwidth to the places it is needed. You can pick up another extension in your home and link in to a conversation already going on, or make another call as if you had two phone lines, or more. No problems with paying for extra lines for your modem, fax, etc. You pay Sprint monthly by how much bandwidth you consumed. That could get pricey. Not to mention you could be constantly connected to the Internet as if through a T1.

Sprint has teamed up with Bellcore and Cisco, and are planning to sell their equipment through Radio Shack, who already carries a wide variety of Sprint products. Bellcore is providing the central software framework for ION's network, in addition to providing consultant services to ensure reliability of the new network. Cisco will provide critical hardware for the system, both in the CO and the home/business. They will also provide the ability of voice over Asynchronous Transfer Mode (ATM) and the ability to connect to other carriers' legacy circuit-switched networks. Several companies have committed to using ION, including Coastal States Management, Ernst & Young LLP, Hallmark, Silicon Graphics, and Tandy. (Hey, remember back in the 80's when McDonalds volunteered to test ISDN?) The city-wide networks were deployed (to the best of my knowledge) last fall in:Chicago, Atlanta, Dallas, Houston, Kansas City, Denver, and New York. The reason these cities were chosen as the initial city networks was because of the existing conditions resident in each of them, including broadband MANs (Metropoliton Area Network) and strong customer bases. Sprint claims its ION lines can carry as many calls as Sprint, AT&T, and MCI currently carry put together. Mmhmm....

Here's how it works: The nationwide Sprint Fiber-optic network is connected to service nodes which in turn connect to the MANs. The fiber-optic network is connected to the Internet and other data networks. The MANs connect homes and small and large businesses all over the city. Every residence/business would have a central hub which connects them to the MAN. A diagram provided by Sprint shows a home having a fax machine, a computer, and a phone line connected to a hub which has a direct line to the MAN. The general layout of the network is a star topology, with the fiber-optic network at the center.

The Future

We can only wait to find out the future of this emerging technology. I will write another article on the possible hackability of ION when the technology becomes more commonplace (especially when I get to use it). The idea of an extremely Wide Area Network sounds very interesting (hmm, how 'bout that Network Neighborhood?), and if the network becomes a commonplace technology, it's our job to find out all about it. It would seem slightly scary to have your phone/fax/modem all hooked into the same line and controlled by the telco. Would you have a choice of ISP's? What are the possibilities for wiretapping? Or packet sniffing? We'll see soon.

My thanks to Vegeta125 for getting me a lot of info on ION, Bioweapon, Cheshire, and Crunchman for reviewing the article.

continued from 39

glitch in the electronic "push screen" teller machines at CitiBank. If you go to a vacant machine and look down at the screen, you will see a prompt to put in your card. Start pushing at random places on the screen. You will notice that they all make the same low beeping noise. However, if you push in the upper right corner of the screen, you will hear a slightly higher pitched beep. Once you've heard the sound, repeat the pushing twice. Then get away. A new screen will pop up asking for the user to put in a CitiBank card. Even if someone tries to do this, nothing will work. Instead, the machine will freeze and make more beeps. Scares the shit out of any unsuspecting person. Luckily though, after about 30 seconds of the "freeze," everything will return to normal. Just a fun little thing I like to do at CitiBank.

errorshutoff

We published this a few years back actually. It's not a glitch but a feature for the visually impaired. It works quite well too. But you need to enter numbers in a slightly different manner. It's fun to figure out so we won't spill the beans here. When you successfully complete a transaction, you get victory music. Defeat music follows all failures as well as all timeouts. Many an afternoon can be spent repeatedly putting a row of ATM's into this mode and hearing the defeat music sequentially going down the line in the midst of confused bankers.

Dear *2600*:

I don't know if this is common knowledge but here goes anyway. I recently got a Nokia 6185 and was moving about the web looking for interesting information on my new phone. I found a review which makes reference to a string that would get you into the field test mode of the phone. I tried it out and let me tell you it offers a whole lot more than a toggle for the field test mode. Here is where the fun starts. The 6185 has two different codes you can setup, a lock code and a security code. The lock code is used to lock your phone, meaning that a locked phone will prompt you for the code if you try to make a call, get into the address book, etc. The security code is used to give you access to various user system settings.

Try this with your own Nokia 6185:

1) Make sure "Phone Lock" is on by going to Menu/Settings/Security settings/Access codes/Phone lock and selecting on.

2) Turn your phone off.

3) Turn your phone back on. It should say "Phone locked" at the bottom of the display above "Menu" and "Names".

4) Selecting "Menu" will trigger the prompt for the lock code.

5) Say you forgot your lock code and you continue to get it wrong when prompted. After the five incorrect attempts you will be prompted for your security code. You forgot that too? Never fear!

6) Key "Back" from the prompt for the security code. You should be back at the main screen.

7) Enter the following string: *#3001#12345#

8) A nice hidden menu will appear with lots of things to look at. We are really interested in the "Security" item so select it.

9) What you see looking at is the current security code for the phone. You can change it or merely memorize it once and for all.

10) Turn the phone off and then back on again.

11) When prompted, incorrectly enter the lock code five times.

12) When the prompt for the security code comes up, enter the security code.

13) The phone is now unlocked and ready for full use.

If none of this worked then you are either doing something wrong, have a different (better) version of the software, or are simply using a different phone. I hope Nokia, Sprint, or whoever is responsible plans to offer a software upgrade that removes this back door. Leaving your phone is pretty much meaningless so be careful out there. As a side note, this should also work with the 6158 although I have not tried it.

Dumah

Dear *2600*:

Just recently, I was exploring the plethora of channels on Cox Basic Cable in South Orange County, CA and I stumbled upon something rather interesting. On channel 117, there was some sort of active line-graph monitor on. No sound, no nothing. Just this moving line graph. It looked like some sort of computerized seismograph program. I turned on the same channel several hours later, and it looked like the same pattern. Probably looped. The same oscillated lines over and over. But every day, the loop changes. I'd like to learn about the computer that puts this through the broadcasting network. What organization would be broadcasting such a thing? Why? Why would it be just a looped pattern of wavy lines? Would you have any idea what this is?

Snot Gnome

We've noticed a similar channel but only when a TV is hooked up without a cable box. Might be a good idea to tape this channel and see when the change occurs. Might also be a good idea to call the cable company and demand to know why there's an alien spacecraft on one of their channels. Something tells us our cable technician readers will be writing us about this one so just stay tuned.

Dear *2600*:

I've had my Qualcomm (QCP-2700) phone for over two years. Twice I've had the software upgraded and now have BH3.109, PRL 231 installed. Millions of these units are in circulation (under different names), and I would like to share what I know, in hopes that someone will write with additional information.

If you turn the phone on, press 11111 (six times), then push the select key. You will go into a diagnostics mode. The screen displays 1) Version 2) Programming 3) Field Debug.

In order to go into Programming or Field Debug, you have to enter a password. I have discovered the default password for the Field Debug screen is 040793 (or 040PWD). This won't work to get into Programming mode.

Once in DEBUG mode, there are more options. 1) Toggle QNC (?). 2) Screen (Changes screen display into Hex values). 3) Test Calls.

Test calls is what I am curious about. Once in DEBUG mode, I have options to make the following types of call: Old8kMarkov, New8kMarkov, New13kMarkov, 13k Loopback, 8k Loopback with an option below that says Start Call. Does anyone know what a Markov type call or Loopback type call is?

Every time I ask someone at Sprint (my PCS provider) or the people at Qualcomm, I get told to stay out of diagnostics mode or I might have to bring in my phone for reprogramming. Why do I have passwords on my own phone anyway? Isn't it *my* phone? Am I paying a license fee or do I not own my own phone?

Shawn

An interesting phenomena takes place with some phones (we've noticed it on Samsungs) when in that mode. On one of the test calls, the phone will redial the last number it tried without telling you on the screen. That phone will ring and the person who picks up will hear a scrambled signal that sounds like R2D2. No kidding. As for the Screen setting, you will also see things in there like signal strength and transmitter identifiers.

Dear *2600*:

I'm not your standard paranoid guy, but what's happened to me seems incredibly... odd.

I recently got to college and noticed that I was behind a set of firewalls. We got laptops that were set up to use proxies via an autoconfiguration script for Netscape. Before I had setup proxies for Outlook on my computer I had wanted to check e-mail in pop3 accounts that are outside the firewalls. In order to do so without knowledge of the proxy servers I decided to use Netscape and sign up for a yahoo account (you can check pop3 accounts with it). What happened next was what seems so odd.

While signing up for a Yahoo account, they requested that I fill out a form that includes a special question that is used for retrieving a forgotten password. They automatically suggest a question, and an answer. This question and answer hit very close to home.

The suggested question was: "What is your favorite pet's name?" and the suggested answer was: "B.J."

I happen to have a dog named B.J. This is an incredibly odd name, nearly one of a kind and thus I conclude that it could not be just a coincidence.

What is Yahoo doing with personal information about me? How did they know it was me if it was my first time using this computer and the first time I used my school network? I suppose they referenced me in a database and I was the only one with my name in their list, but it's not an uncommon name.

Paranoia? I don't know.

Dissolution X

We do.

Dear *2600*:

As I was listening to the October 1988 edition of *Off The Hook*, I realized that while I am only 15, I really do feel like I am part of something special. When I think about computers, I think about them as "a gateway" to another world. I think of them as marvels. I can sit there for hours pondering over the internal workings of a Commodore 64, or a Vic 20, an 8088 laptop, 186, 286, 386, and so forth and so on. I've noticed today in the "computer" world, there are many people, young, old, new, who don't understand, but also believe they do. They think that "hacking" is composed of loading up their AOL, or any ISP connection for that matter, and firing away a nuker, eggdropper, or some other exploit. They don't understand that a hacker is not always someone who is malicious, or someone who only goes to destroy, or ruin someone's day. They don't know that a real, true hacker is someone who wishes to understand how something works... who wants to dive into the depths of how this functions, how part A talks to part B, or how the computer can interpret input from us, in our human language, convert and understand it in its own language, whether it be strict Assembly, Binary, Hex, C, C++, Java, visual basic, Pascal, Fortran, Perl, Cobol, and so forth.

I am only in the 10th grade, but already I know that I do not want to go into this world as one of the people who don't know A from B, B from Q, 17 from 35, and 00110 from 4e6. I am not exactly sure why I felt the need to write to you, but I needed to vent my voice. I want to dive into the depths of science, computers, how they work, how they will work. How the phones work. I don't want to destroy, I don't want to break, I only want to learn. I think that is what is wrong with society today. The American media has shown hackers as people who sit in their room all night, doing nothing but squinting at their monitors, trying to mess up someone's computer.

Graphix

So few people retain this sense of wonder that really is an essential part of appreciating technology. If you ever reach the point where you can talk to someone on the phone or over the net and not realize how incredible the whole process is, you've lost something really important.

Dear *2600*:

In 16.2, Flite wrote "What the hell is the background of Issue 16 I supposed to be?" Your response was "Reflection. Surprise. Terror. For the future." That line is from a *Babylon 5* episode in which Kosh said those words to Talia Winters. I just thought that was a perfect response on your part. I also want to say that this Free Kevin crusade you have started is the most inspiring

thing I have read about in a long time.

Websurfer

At that is one TV show that has been a great inspiration to us, we're glad someone picked up the reference. Now if only someone would pick up "Crusade."

Questions

Dear *2600*:

I would like a little more info on the ice.2600.net server. Isn't there a number that my modem must dial to access the server? And do you have any pointers how to switch servers back and forth. This is very necessary because I have to share the computer with other "family" who would absolutely freak if they knew where my interests lay (needless to say, I use Magic Encryptol Folders to keep my personal files personal). I am trying to stay inconspicuous and am very interested in using the hacker server when I am actually online.

Val

You must already be connected to the net before you can use the ice service. It works exactly the same as any other ice server anywhere in the world. All you have to do is replace or add our server name in whatever program you access ice from. Simply connecting to it is not going to get you in trouble since it's rather indistinguishable from any other ice server.

Dear *2600*:

I have a question. I have two separate lines for my home, and on my computer line sometimes it will say "the computer you are dialing isn't responding" so I plug the phone line into my phone and there are two women talking on my line and they can hear me. I was wondering what is going on?

Infinet

It's a stab in the dark but we'd guess that your phone line really belongs to someone else. Either that or their phone line belongs to you. No matter how you look at it, the same phone line is showing up in two places. The phone companies do this all the time.

MTV

Dear *2600*:

I live among the MTV race, or so I like to call them. Most of us reading this magazine know the type: Harley wearing, trend loving, brown nosing, spoiled popular kids. Most schools probably have 25 percent of these kids, give or take a couple. Well, my school was around 90 percent. The remaining 10 percent are considered low life scum. As I read the article on the *2600* site (www.2600.com/news/1999/1019.html) about MTV's "True Life: I am a Hacker," I realized that everyone at my school now thinks that they can all die at the stroke of some keys.

I decided to post the article around school to inform everyone what a crock of shit it was. Bad idea. It landed me in the principal's office with two Saturday detentions. They asked if I had anything to do with it and I replied that I thought it would be an informative article on the misleading media controlling our youth. They told me that it was a pro-terrorist act and against school policy. Then they found three copies of *2600* in my shoulder bag. They said that it was unjustified reading material and they proceeded to confiscate it. Unjustified? What the hell was that supposed to mean? Did they think what they were doing was justified? Anyway, I told them that it was research for my computer class because we were learning about servers, and then they banned me from using a computer on campus.

I went to my detentions and was doing fine for a week until my fourth period English class. I read a poem about weird smells to the class, once again earning myself two Saturday detentions, which I refused to go to. Principal's office again. This time they called my parents and told them I was guilty of insubordination. After I explained the situation to them, they thought it was the stupidest thing they had ever heard of. My mother called the principal screaming things meant to be written in asterisks.

Monday morning, as I walked into my geometry class five minutes late, everyone turned around and stared at me. What the hell was going on? I later found out that my teacher told the class not to listen to my "preaching" and to ignore my pamphlets.

Well, now I am at another school (I was suspended for bringing my laptop to school so I left, again). I hope that the Constitution is one day burned since there is no meaning to it anymore when you can't post that a TV show wrongfully portrayed hackers in the world.

Oh, by the way, after I left someone changed every computer screen background and screen saver to say "Free Eddie."

Skanarchist
(Fiddle)

Dear *2600*:

I want to offer a bit of mass activism regarding your recent deception at the hands of MTV. Your first mistake was ever trusting the media establishment (or in MTV's case, something pretending to be part of the media establishment) and anyone who thinks that she can do investigative journalism while wearing camouflage pants. I am sure you have realized this by now, so let's move on. The question is: How do we overcome the issue of generating publicity for important issues (i.e., Kevin Mitnick) while still retaining control of the message? From my experience, you have two options: Hold something over their heads to ensure compliance (i.e., refuse to sign releases until you see the final cut) or control the means of production. You would have been better served by the latter, making your own documentary and then offering it to MTV and anyone else who would be interested, airing it yourselves via the web or cable access, and offering it to network news as a clip for those 15 second news stories that they love so much. I must admit I am surprised the hacker community would allow someone else to do their talking for them.

i hall

There are already people doing their own productions. But it isn't wise to isolate ourselves completely from the media since they will then be assured of doing a bad job every time. Had we not tried to help them, we're sure some story would have come out except we wouldn't have realized how much they didn't care about the truth. It was an unfortunate but necessary lesson.

Dear *2600*:

My friends told me that there was a show on MTV about hacking a few weeks ago and started talking all of this shit. It was so funny to see that my uninformed friends thought they could be hackers. They threw these stupid facts at me and my amusement turned to anger. I realized that the bullshit that MTV was producing was setting the hacker community back very far. It was hard enough to explain anything about hacking to my friends in the first place, but now it's almost impossible because they don't believe MTV could actually lie. So this really sucks.

techx3

Dear *2600*:

I would like to say that MTV did the hacker community a great injustice. They really took advantage by using young hackers to do the whole documentary and exploiting their big egos. I really was disappointed about the viewing time of the UOpit which seemed to be the most interesting part but it only lasted less than a minute.

Also I'd like to know if *2600* will ever have an online shop to subscribe and purchase T shirts and *2600* merchandise. Will you guys ever expand your merchandise to include a *2600* coffee mug which would be cool for my desk at work!

UncleFhester9600

If we get a design that doesn't make us feel like idiots, we'll probably give it a shot. As for the online store, as it happens we just started one on our web site which means you can order subscriptions, back issues, shirts, etc. without having to waste time and postage mailing letters. And things generally arrive much faster this way too.

Barnes & Noble Memo Found?

Dear *2600*:

I hate to admit it, but I took a job jockeying the espresso machine at the Barnes & Noble location in North Richland Hills, Texas. I discovered that I make a great cup of coffee, but I never expected to discover this cute little memo posted on a bulletin board in the back. After scanning over it and picking my jaw up off the floor, I snagged it off the board and stuffed it in my pocket.

I think that this memo might explain many of the seemingly random instances of readers under the age of 18 being told they cannot purchase *2600*, and the other various cases of *2600* never showing up on the shelf.

Memorandum

TO: *All Stores*
FROM: *Tom Tchorzsky*
Date: *October 27, 1997*
Subject: *Community Standards*

The protests, letters, and phone calls regarding the works of Jack Sturgis, David Hamilton, and Sally Mann continue around the country. A few pockets of extreme activists exist in some markets, while other markets have experienced no activity at all. All stores have responded quickly and professionally resulting in few confrontations or emergencies.

Over the years we have experienced similar activity with books such as "Satanic Verses", "The Anarchist's Cookbook", and "American Psycho." Being purveyors of the written word and trustees of the First Amendment is not without its complexities. Though all of our customers welcome and appreciate our broad assortments, many of them also ask that we apply discretion in our assortments regarding individual "community standards" in each of our markets.

Keep in mind that we will not categorically remove any book from the shelves, nor will we violate any laws up to and including the books we sell. If any court of law determines any of our books to be in violation of Federal, State, or Local legislation, we will remove them from our shelves. In the absence of such a finding we are entitled, under the First Amendment, to offer for sale any book requested by our customers.

The selection and display of books for sale within our stores is a little more complicated. Many of our communities have specific laws regarding the availability and display of some of the books we sell. In some communities, the laws are specific enough to state by name that "Playboy" and "Penthouse" must be secured from open sale and not available to minors. In the face of the variables, if you believe that any book we send you is not appropriate to the laws and standards of your community, you are encouraged to place it in a secure location and in some instances remove it from the shelves of your store. We will still order any book in print requested by our customers and, as always, books containing sensitive material will not be sold to anyone under the age of 18. Certainly, if there are books in your store that you believe to be beyond the tolerances of your community, be sure and communicate your actions to your district manager.

Thank you again for all your support and continued good judgment in the handling of this issue. Should you have any questions, please contact your district manager, regional director, or myself.

You guys getting this? Any slack-jawed yokel working at B&N (and believe me, there are plenty of them) can decide to implement his/her own flawed moral judgment and take *2600* off the shelf and put it behind the counter so no one under 18 can purchase it. For that matter, this inbred moron could go rack the whole stack of

mags in the back, to be stripped and sent back to the distributor because this underachiever, $6.50 an hour month breather might think that the material is too sensitive for his/her community. Not to mention the bad name they give to innocent materials such as *2600* by grouping them with the likes of pedophilic photography, racial bigotry, and other such truly disturbing publications. If I owned a company the size of B&N, I must assuredly would not allow the lowest employees on the corporate ladder to make any decisions for my company, much less decisions that could potentially enrage my customers. Pretty retarded way to run a book store, if you ask me.

Mangoburn

We've contacted Barnes and Noble concerning whether or not this memo actually was circulated. If it was, it could certainly explain some things, not only for us but for a whole host of other publications. We'll wait to hear what they have to say on the matter. We like to think that the vast majority of stores have people like the following writer in positions of power.

Dear *2600*:

A customer called our store, the Barnes & Noble in Muskegon, Michigan tonight and told us that someone had written a letter about our store in your magazine. We read it and wanted to reply. We have sold your magazine in our store since it opened three and a half years ago. It seems that most times we sell out of your magazine. I'm not sure who that guy talked to, but obviously it was someone who didn't have a clue. We just wanted to let you know. Thanks!

Dawn Bates
Bookseller at B&N
Muskegon, Michigan

Fun Stuff

Dear *2600*:

Found something quite interesting, amusing, and well, all around funny today. While going to an eye appointment today at the local military hospital (I am a military brat, yay), I heard on the PA that "we are now in ThreatCon Bravo." For those of you who don't know what ThreatCon is, it's Threat Condition... the base I was on has been at ThreatCon Alpha since the Gulf episode. The higher in the alphabet, the worse conditions are. Anyway, ThreatCon Bravo is supposed to be pretty not good. This kind of spooked me a bit, when I remembered that this week was some sort of "prepare for the worst" week. Making my way over to the exit, I heard this about three more times. It got me thinking. I changed direction and headed to my father's office. Before I could even open his e-mail folder, I heard "d d d ling", like the old Windows startup sound (scary, I am a Un*x guy). This was his auto-email-notify. I opened the message and here's what I got:

"WE ARE RAGE (REBELS AGAINST GOVERNMENT ENTITIES). WE OWN YOUR SYSTEM. WE ARE BREATHING DOWN YOUR NECKS. YOU ARE OURS."

I almost broke out into a laugh when I thought the hospital's system had been breached. Then I finished reading the message:

"THIS IS A SECURITY EXERCISE FOR THE HOSPITAL."

Oh well, it was fun. A few moments later, another e-mail arrived saying, "When in ThreatCon Bravo, look for any suspicious characters and report them to security." Considering I was looking kind of suspicious (little dude, black baggie pants, antigovernment shirt on... what a day to choose to wear that!), I bolted for the door. Good to know the army is scared. Love your zine.

Slack Packet

Stories of the Past

Dear *2600*:

Enjoy your magazine! Thought I'd reminisce a little. I learned to program FORTRAN IV on punch cards back in 1980 at a junior college. When I got to a University, I got an account (wow), and was able to program through a remote terminal. I was an engineering student and spent many hours into the early mornings programming and looking through areas I could get into. The only hack I ever did was when a slow-witted student used one of the engineering terminals and left it without logging off. I happened upon it. I wrote a batch file that executed upon startup the next time he logged on. The batch file executed a program that told him to remember to log off before leaving the terminal. A few days later I found another terminal that someone had not logged off of. When I checked the account number I found out it was the same account as the last one I found! I wrote another batch file that ran at login. It was a bit more exciting. Essentially it said, "Close your account, dumb-shit." I laughed to myself and forgot about it. Not two days later I found the same damn account open again! So this time I wrote a batch file that looked exactly like the login screen and asked for his account number and password. This second login was my hack. It sent the password to a dummy account I had. (I knew that the sysop could track me down if I used my own account. I had six spare accounts, some I had inherited from students who had graduated and never told the computer manager they had left. Things were a lot less strict back then.) Anyway, the account owner didn't even suspect a problem even though he had to enter his password twice (big clue that something is wrong). As soon as the password got sent to me, I had the batch file change the password and log off. I passed the account number and password around the engineering department and we used the account to poke into where we were not supposed to. We were kind enough to leave the files intact. It only lasted a few days before the sysop changed the password again and I lost my play account. I played more pranks on other engineering students and anyone who happened to leave a terminal open without logging off. But I never stole another account. Anyway, keep up the good work and remember to have fun, but do no harm.

Brien

Understanding Microsoft Exchange

by PayLay
paylay666@yahoo.com

Microsoft Exchange Server is one of the most popular and widely deployed groupware and messaging servers around. It's also very easy to install and configure, so a lot of know-nothing jackasses are becoming Exchange administrators overnight. Typically, these mail servers are not very secure and often misconfigured. Whether you are a hacker or an Exchange administrator, there is one golden rule of security: NT is only as secure as the infrastructure; Exchange is only as secure as NT. Both rely on an informed and competent system administrator.

The purpose of this article is to introduce the curious to Microsoft Exchange, how it works, and its vulnerabilities. I am not going to teach you how to hack into NT; volumes could be written on it's exploits.

Understanding Exchange Server

Microsoft Exchange Server is a groupware and messaging tool, built for medium to large corporations. A lot of smaller companies also use it because of the ease of installation and native support for Outlook mail reader. Like all Microsoft products, it uses proprietary protocols and mail transfer methods. But it also supports most major standards of mail transfer and the like. "Out of the box" Exchange supports many protocols, including these: X.400, X.500, LDAP, SMTP, POP3, and IMAP4. The X.400 and X.500 connectors can be quite fun, but that is a whole other article. Internally, it supports connectivity to other mail systems, such as MS Mail, Notes, CC:Mail, Groupwise, and SNADS. For Internet connectivity, it has a built in SMTP server.

Connection and Authentication

Exchange Server supports four ways to connect to it:

1. Exchange Client. "Exchange" client is a MAPI program that can natively connect to an Exchange server. For a long time it was only the Exchange Client which shipped with early versions of Exchange and Microsoft Outlook 97/98/2000. These clients use NT Authentication, meaning you have to have an NT account on the server/domain with appropriate permissions in order to connect. Recently, HP announced that OpenMail for HP-UX and Linux supports Exchange server connectivity. I haven't seen it so I can't tell you how it works, but the Linux version sounds like something fun to hack around with.

2. HTTP. Starting with Exchange version 5.0, Exchange has a feature called Outlook Web Access. A server equipped with IIS3/4, Active Server Pages, and Exchange 5.0 and above can present the Outlook interface through a web browser so users can access their mail. Challenge/Response authentication is the default, but it requires IE. Most administrators step the authentication down to clear-text so Netscape users can access their mail. This is a common mistake a lot of admins make, sacrificing security for usability. The default path to Exchange's OWA is "/". A lot of companies allow anonymous access to public folders. If you poke around long enough, a lot of information can be gained from reading public folders. A side note: OWA uses LDAP to do queries on the Global Address List. If you can access OWA from the Internet, chances are they have anonymous LDAP enabled. With a LDAP-enabled mail reader, you are browsing their corporate email list in no time. In most Exchange sites, email address = NT username. 'Nuff said.

3. POP3. Exchange allows POP3 clients to connect to the mail server. If an administrator enables this, they usually enable clear-text authentication. I have noticed most admins would rather just enable clear-text than hassle with upgrading mail clients.

4. IMAP4. See POP3. Same authentication.

Now that I have laid out various protocols, it's obvious there are various ways to connect to Exchange from the Internet. Microsoft has had their share of security problems with Exchange, which were subsequently fixed by an Exchange Service pack or hot fix. I have been working with Exchange for years now, and I have not once been to a site that had the latest service pack or hot fix. So, the first step in understanding Exchange's vulnerability is understanding what build you are working with.

Two ways to get this info; look at the mail headers:

[snip] **with SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2232.9)**

or telnet into Exchange on port 25:

[snip] **220 mail.paylay.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2232.9) ready**

Build	Exchange Version
4.0.837	Exchange 4.0
4.0.838	Exchange 4.0 SP1
4.0.993	Exchange 4.0 SP2 (also referred to as Exchange 4.0a)
4.0.994	Exchange 4.0 SP3
4.0.995	Exchange 4.0 SP4
5.0.1457	Exchange 5.0
5.0.1458	Exchange 5.0 SP1
5.5.1960	Exchange 5.5
5.5.2232	Exchange 5.5 SP1
5.5.2448	Exchange 5.5 SP2

Exploits

Obviously, if you come across a server that is using a very early build, chances are they haven't bothered to install any NT or IIS service packs. This is a sad fact I find completely laughable. Give me my Palm and Palm modem and 10 minutes on an Exchange build 2232 on NT SP3 and IIS out of the box, and I will be perusing payroll, tax, or bribe information or just looking at some jerk's corporate sales contacts or whatever. If you are interested, do a little homework on general NT and, more specifically, IIS exploits and you will find a lot of useful information. Some common, open holes in an Exchange Server:

1. A lot of dumb-ass VP's want to check their e-mail from their Palm and cell phone from a desert island using their *own* ISP. Because a lot of admins are dumb, lazy, or scared of their boss, they have allowed anonymous access into the SMTP portion of Exchange. Check this first.

2. Exchange's SMTP connector has a feature that disables mail relaying. A *lot* of companies have this feature turned off because they probably don't understand what mail relaying is. Heh, they probably think it's a *good* thing. So check into this next.

3. If the build is 5.5.2448 or below and they have mail relaying disabled, there's still a way around it. If the e-mail is sent using what's called "Encapsulated SMTP", a way for Exchange to send mail to another Exchange Server via SMTP, you can relay mail because it allows relaying if the mail appears to be coming from another Exchange server. Microsoft has a hot-fix for it, but most companies run NT Service Pack Nothing, so check this out.

4. Exchange uses NT authentication for mailboxes, so exploits used for NT passwords can be applied to Exchange. Hack the Administrator password and you just hacked the Administrator mailbox.

5. Any mail standard Exchange uses (IMAP4, POP3, SMTP, etc.) is, well, standard. So the general rules when dealing with those protocols also apply to Exchange.

Under the Hood

Exchange has what's called a Service Account. This is the NT account that Exchange uses to send/receive mail, stop and start services, and perform other Exchange-related duties. This account should be the most secure account on your mail server. So, let's find out what the Service Account user name is:

Click on Organization\Site\Configuration\Server and bring up the properties for the current server, then click on Permissions. There is a box titled "Windows NT Accounts With Inherited Permissions". Scrolling through the permissions list, there is a set of permissions called "Service Account Admin". A smart NT administrator would have a dedicated account that is *never* used to log in with, and this account would have a *very, very* strong password. Why, you ask? Because an account with this set of permissions is GOD. A Service Account Admin can do anything, read anyone's mail, contacts, calendar, journal, tasks, and public folders. You can send mail *as* them, receive mail, set incoming mail rules, forward mail, filter mail to another mailbox, *anything*. You can set up a filter and rule on the CFO's Inbox that will copy all mail with the words "Confidential" or "finances" in the body, and have it automatically delete out of Sent Items so he never knows. With Service Account access, the possibilities are endless.

Now, your next question is: which is the Exchange Service Account in the user list? Good question - a jack-hole administrator would make it the default NT account - "Administrator" or he thinks he is gonna fool the hackers and name it "QrG6fW1". I usually call mine "Joe Rodriguez" with the username "joer". Something obviously *not* a service account. Another good place to start is if you have access to the NT user list and the Exchange Global Address List, start cross-referencing names. Some admins may have created a Service Account mailbox, but hidden it from the address list. So, figure out what NT accounts don't have mailboxes. You may be looking at some kind of service admin account, Exchange or otherwise. Of course if you have weaseled yourself into some kind of admin access in the NT domain, but you don't have access to the Exchange server, see what services are running on Exchange. With some crafty NT Resource Kit tools and some NET commands, you will be able to bring up properties for services. With the "Start Up" properties for *any* Exchange service, who has "Log On As" permissions? You have just discovered one Exchange Service Account username. It may not be the only one, but it is a start.

This is a good basic introduction to Exchange. It is just as much a hacking tutorial as it is a how-to guide for Exchange admins on how a network ought *not* to be designed.

Continued from Page 5

The answer has been staring us in the face for some time. And Seattle was the first opportunity to apply it on a somewhat massive scale.

The technology that has been developing over the years is unquestionably of great benefit to whoever decides to make use of it. The relatively open architecture of the Internet lends itself to a great variety of applications, not just for those with the most power. That is its magnetic allure and it's also the reason everyone in authority is scared to death of it. The net represents the true potential of the individual and individuals are the most formidable enemy of any oppressive regime.

As the crowds were gassed and shot at, the mass media looked elsewhere. They found a small group who, in the mayhem, had taken to vandalism, smashing windows and torching cars. This became the only "violence" most Americans saw on their televisions. Businesses were the victim, individuals the cause. Newspaper chains ran editorials condemning this "violence" against property, ignoring the assault on the people, and endorsing the continued existence of the WTO. Anyone who was surprised by this simply hadn't been paying attention. When you look at how power has been consolidating in recent years, this kind of coverage makes perfect sense.

But then there was the net. The same net that is encroached upon daily by those in power. The one that governments around the world continue to try to regulate. It was the Internet that finally broke through the manipulation and allowed the world to see, firsthand, what was actually happening.

Strategically placed webcams showed everyone what was really going on in the streets. Mailing lists and newsgroups allowed anyone to instantly write their experiences and get them out to the rest of the world. Any person with a tape recorder was able to go out and get sound, then encode it so that people from anywhere could listen. Almost as many people managed to do the same thing with video. Within hours, dozens of these independent media pieces were traversing the planet, all without control or censorship. And, in one of the most shining examples of free speech we've witnessed in a long time, a "pirate" radio station broadcasting live from the streets of Seattle was able to get its signal streamed onto the net so that people anywhere could listen to its weak but captivating signal. (We put quotes around the word "pirate" because it seems ironic that such free speech on the public airwaves would be illegal while it's perfectly acceptable for one single corporation to control close to a thousand far more powerful stations.)

You probably didn't hear about any of this in the mainstream media for the same reason you didn't hear about what Kevin Mitnick actually did to warrant being locked away for five years. Why dwell on the psychological and physical torture that Bernie S. endured, all because the Secret Service was mad at him? Wouldn't more ad space be sold if Zyklon were shown as an electronic terrorist rather than a simple juvenile delinquent? It's far easier to portray events with the smoke and mirrors we saw in a recent MTV slander piece on hackers as well as so many other corporate media fiascos. The facts only serve to complicate matters and muddy the message. And people are stupid, after all. All they want is to be entertained and nothing stands in the way of that more than the truth. Right?

The tide has turned. It may take some time, but it seems obvious to us that not everyone is buying into the propaganda. We'll see many more individuals whose punishment far outweighs their crime and we'll see the media distort the facts time and time again. But one thing we know we have now that may be the biggest contort of all - awareness. That, combined with the technology that we must never let them take away, will be enough to start reaching others.

Statement required by 39 USC 3685 showing the ownership, management, and circulation of *2600 Magazine*, published quarterly (4 issues) for November 15, 1999. Annual subscription price $18.00.

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

	Average No. Copies each issue during preceding 12 months	Single issue nearest to filing date
A. Total No. Copies Printed	55,000	60,000
B. Paid and/or requested circulation		
1. Sales through dealers and carriers, street vendors and counter sales	47,500	55,000
2. Mail subscriptions	2001	2122
C. Total Paid and/or requested circulation	49,501	57,122
D. Free Distribution by mail (Samples, complimentary, and other free copies)	450	450
E. Free Distribution outside the mail, (Carriers or other means)	200	200
F. Total free distribution	650	650
G. Total distribution	50,151	57,772
H. Copies not distributed		
1. Office use, leftovers, spoiled	4849	2228
2. Returns from news agents	0	0
I. Total	55,000	60,000
Percent paid and/or requested circulation	99%	99%

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

MARKETPLACE

HAPPENINGS

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

FOR SALE

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

HTTP://PAOLOS.COM since 1996. We offer lockpicking and auto entry tools, confidential trade publications, survival tools and goods, an exciting line of switchblades, some priced as low as less than $25, and a complete line of super-realistic Airsoft guns. Danger: do not brandish these guns in public, you may be arrested/shot. We guarantee what we sell UNCONDITIONALLY for 30 days, in addition to factory warranties, and will beat the competition's prices on anything! No "spy store" or "Y2K" hype here. Visit us to post messages to our discussion board, add your e-mail to our mailing list, or place an order with our easy-to-use catalog! We ship internationally, and only sell to qualified customers.

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

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

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

LEARN NUMBER BASE THEORY the easy way. Booklet + DOS diskette. $17 ppd, Low E. Jeppson, 138 S 300 East, North Salt Lake, UT 84054.

REAL HACKER MOVIE in production. We want your input about Y2K. Email: movie@jnq2020.com. DoomsDay Scenario coming soon!

TECHNICAL BOOKS AND HACKER FICTION: OpenVMS manuals, C, networking, Cuckoo's Egg, etc. Send e-mail for complete list to: EthBooks@yahoo.com.

Y2K MUST HAVES: Tired of all the Y2K hype? Or do you want to show you survived it with a grin? If you answered yes to either you need to order your "Y2K - Just hype it" t-shirt or your "I Survived the Y2K Bug" t-shirt. These white with black print shirts are a must have for all hackers etc. to show your true feeling of Y2K. We also offer a "Life is a Progress Indicator" t-shirts for all computer users who know what it means to spend hours and hours in front of the screen. To order: Please specify which shirt(s) you would like and quantity. They come in L or XL for only $16 plus $4 S&H. Please send check or money order with mailing address payable to: Curt Baker, PO Box 50425, Sparks, NV 89435. Allow 4-6 weeks for delivery.

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

PEOPLE WITH ATTITUDE. Check out the political page at the Caravela Books website: communists, anarchists, Klan rallies, ethnic revolt - all at http://users.aol.com/caravela99 - and a novel, "Rage of the Rose" by Bert Byfield about a 15 year old blonde girl who learns the art of war and becomes a deadly Zen Commando warrior - send $12 (postpaid) to: Caravela Books QE393, 134 Goodburlet Road, Henrietta, NY 14467.

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers unCyclopedia '99 - 12,371 files, 681 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, 155 911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

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

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 25 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M.L. Shannon, ISBN 0-87364-972-9, 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1307, Boulder, CO 80307 and by special order from Barnes and Noble.

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

HELP WANTED

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

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

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

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

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

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

I AM LOOKING FOR ASSISTANCE in cracking alphanumeric password protected MS Access files. Please send all info to laptop2000@yahoo.com. Your help will be greatly appreciated. In return, anyone needing info on WHCA (The White House Communication Agency), I will be happy to lend assistance with copies (or fax) of all ground floor (T1 through OC128) to DC metropolitan area or other documents.

PROFIT FROM YOUR TALENTS! Computer hacker wanted for confidential and lucrative assignment. Experienced only. No newbies please. Must leave clear message with phone number and email address plus best time to reach you. Call Steve 212-864-0648. Message for Miles: answering machine erased your number! Please call again.

WANTED

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

I'M LOOKING FOR THE ORIGINAL OFFICIAL TAP MAGAZINE/NEWSLETTER. Contact me if you have any information regarding the original TAP phreaking magazine/newsletter. I suggest you provide the condition of the magazine/newsletter and the price that you would want for it when e-mailing me at menace256@hotmail.com or Icq 13693228. I want the ORIGINAL copies only.

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

SERVICES

SUSPECTED OR ACCUSED OF A CYBERCRIME IN THE SAN FRANCISCO BAY AREA? You need a semantic warrior committed to the liberation of information who specializes in hacker, cracker, and phreak defense. Contact Omar Figueroa, Esq., at (800) 966-5841 or (415) 986-5591, at omar@alumni.stanford.org, or at Pier 5 North, The Embarcadero, San Francisco, CA 94111-2030. Free personal consultation for 2600 readers. All consultations are strictly confidential and protected by the attorney-client privilege.

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

ANNOUNCEMENTS

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

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

Personal

LOOKING FOR NEW FRIENDS. Am in the Corruption Center of America (Corrections Corporation of America) prison doing a skidbid that's taking too long. Need stimulation and information. Am WM 5'10", brown hair, brown eyes (for the ladies). Used to go as Admkirk on irc. Bored out of my mind and looking to make a connection. Steven Letak, #00001-AIR9017s, Diamondback Correctional Facility (CCA), P.O. Box 780, Watonga, OK 73772-0780.

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

ONLY SUBSCRIBERS CAN ADVERTISE IN 2600! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgement 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: 3/1/00.

ARGENTINA

Buenos Aires: In the bar at San José 05.

AUSTRALIA

Adelaide: Outside Sammy's Snack Bar, on the corner of Pirie St & Pulteney Streets, 6 pm.
Brisbane: Hungry Jacks food court, Queen St. Mall (RHS, opposite Info Booth), 7 pm.
Canberra: KYs Internet/Reality Cafe, 11 East RA Lane, 6 pm.
Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.
Perth: The Merchant Tea & Coffee House (Murray Street), Meet outside, 6 pm.
Sydney: Hotel Sweeney's Internet Cafe (top floor), corner of Clarence and Druitt Streets, 6 pm.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BRAZIL

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

CANADA

Alberta

Calgary: Eau Claire Market food court (near the "milk bar").
Edmonton: Sidetrack Cafe, 10333 112 Street, 6 pm.

British Columbia

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

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street, 7 pm.
Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000, Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.
Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.
Leeds: Leeds City train station outside Sam Pancho's. 5 pm.
London: Trocadero Shopping Center (near Piccadilly Circus) downstairs near the VR booth. 7 pm.
Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peter's Square. 6 pm.

FRANCE

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

GREECE

Athens: Outside the bookstore Papasotiriou on the corner of Patission 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 entrance), Roppongi (by Sunday Mart).

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 Cafe, Bar, Every Friday, 7 pm.

RUSSIA

Moscow: Burger King [illegible] Telegraph Agency of Russia/Telegraph Agency of Soviet Union) - also known as "Informacionnoe Agentstvo".

SCOTLAND

Aberdeen: Outside St. Nicholas Church graveyard, near the Commerce entrance [illegible] store. 7 pm.
Glasgow: Central Station, payphones next to Platform 1. 7 pm.

SOUTH AFRICA

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

UNITED STATES

Alabama

Auburn: The Student lounge upstairs in the Foy Union Building. 7 pm.
Birmingham: Hoover Galleria food court by the payphones next to Arby's. 7 pm.
Tuscaloosa: University of Alabama, Ferguson Center by the payphones.

Arizona

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

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

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

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Myers: At the cafe in Barnes & Noble.
Miami: Dadeland Mall on the raised seating section in the food court.
Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Manchu Wok. 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: Arts' Tree Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 6 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: Screenz, 2717 North Clark St.

Indiana

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

Kansas

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

Kentucky

Louisville: Barnes & Noble at 801 S. Hurstbourne Pkwy.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & Swensen's Ice Cream, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.
New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting into the phone.

Maine

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

Maryland

Baltimore: Barnes & Noble cafe at the Inner Harbor.

Massachusetts

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

Michigan

Ann Arbor: Galleria on South University.

Minnesota

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

Missouri

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

Montana

Butte: Butte Plaza Mall on Harrison Ave. in the JC Penney food court.

Nebraska

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

Nevada

Las Vegas: Palace Station's Oyster Bar, Sahara & Rancho. 8 pm.
Reno: Meadow Wood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

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

New Mexico

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

New York

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

North Carolina

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

Ohio

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

Oklahoma

Oklahoma City: Shepherd Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9520, 9228, 9201, 9404.
Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Brown Sugar, 402 NE 3rd St.
Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

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

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

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

Texas

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

Utah

Salt Lake City: ZCMI Mall in the food court.

Washington

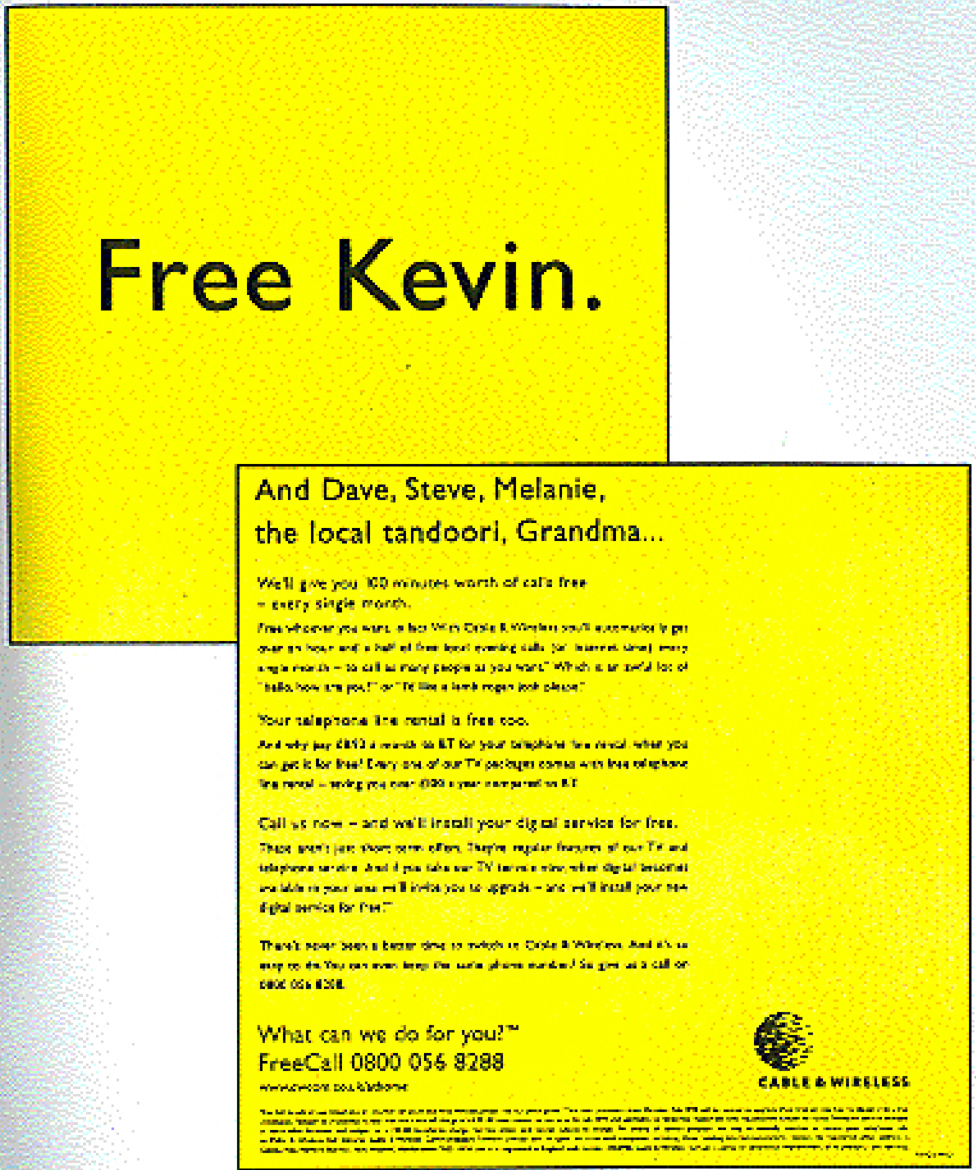
Seattle: Washington State Convention Center, first floor.
Spokane: Spokane Valley Mall food court.

Wisconsin

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

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

FREE KEVIN Sightings



Looks like our campaign has gotten successful enough for Madison Avenue to take notice. Or whatever the British equivalent of Madison Avenue is. This comes from a recent mailing blitz organized by Cable & Wireless. It's so nice to have one's ideals commercialized.

Send Your Photo Submissions to:
2600, PO Box 99, Middle Island, NY 11953 USA